UNIVERSITY
OF TASMANIA

Safe Ports in the 21st Century:

Australian port resilience

By

Captain Victor Robert Justice

MBA (Maritime and Logistics Management) University of Tasmania

Supervisors: Associate Professor S. Cahoon; Associate Professor B. Brooks

Submitted in fulfilment of the requirements for the Degree of a Doctor of Philosophy, University of Tasmania, November 2018

Declaration of Originality

This thesis contains no material which has been accepted for a degree or diploma by the University or any other institution, except by way of background information and duly acknowledged in the thesis, and to the best of my knowledge and belief no material previously published or written by another person except where due acknowledgement is made in the text of the thesis, nor does the thesis contain any material that infringes copyright.

……. Victor Robert Justice, 16 November 2018

Authority of Access

……. Victor Robert Justice, 16 November 2018

Abstract

Australian ports are crucial to the well-being of the national economy and the support of global trade. During 2015-16 Australian ports enabled 1.6 billion tonnes of two-way cargo throughput, representing AU$420 billion in value and approximately 15% by weight of global trade. A prolonged disruption to Australian port operations threatens multiple nations' economies and related supply chains' effectiveness. Port business continuity is important for these reasons, but few studies examine Australian port management within the context of operational vulnerabilities to evolving and unpredictable hazards, and port risk management effectiveness in treating the uncertainties and unknowns of high consequence disruptions. Conventional risk management focuses on known and quantifiable risks, but ports are increasingly challenged by a dynamic and turbulent risk environment associated with unknown, unpredictable hazards and increasingly severe natural disasters. More is required from port decision-makers than conventional risk management strategies and capabilities, and this thesis explores whether a capability gap exists, and what might be required to enable enhanced risk management capabilities.

This thesis examines Australian port operational vulnerabilities from a systemic perspective, encompassing multi-layered networks of internal and external stakeholders including those within the port's hinterland, and the interrelated and interdependent port users within Exclusive Economic Zone waters. The primary research question (PRQ) investigates the underlying risk management concepts and practices that might result in safe port outcomes for Australian intermodal shipping operations, namely, *how does the port manage risks and consequences arising from low probability/high consequence disruptions?* To investigate the PRQ in finer detail, three secondary research questions (SRQs) were developed, as follow:

SRQ1: How do ports currently manage risks and unknown unknowns arising from disruptive events?

SRQ2: What do ports need to change in their practices to become more resilient? and

SRQ3: How might ports operationalise resilience to best manage/overcome risks and unknown unknowns arising from disruptive events?

The empirical research evaluates port risk management effectiveness, and preparedness to meet present and near-term future risks. The secondary research questions examine the state of port-centric resilience knowledge and its application, and what influences, drivers and impediments might affect the operationalisation and enhancement of Australian port resilience.

A mixed methods research approach is taken in designing and analysing a web-based survey of high level and authoritative Australian senior port managers. Of Australia's 27 State government authorised port management organisations, 54 senior managers holding CEO, Harbourmaster and head of department appointments returned 37 valid responses to 28 primarily closed-ended questions. The survey is limited to Australian port managers because this narrow research focuses upon the port's importance and reliability within the national critical infrastructure system. Questions are logic-grouped across themes broadly encompassing management demographics, port hazards and vulnerabilities, risk management and business continuity, and operationalisation aspects of resilience. Quantitative data analysis is performed to undertake non-parametric tests and descriptive statistics, while qualitative data analysis addresses open-ended survey questions. Data analysis findings confirm from self-reports that Australian port managers are capable when managing high consequences risks of a tangible nature – where physical evidence of both the hazard and the hazard outcomes are clear – but less so when a hazard involves uncertainties and unknowns emanating from technological or human threats. Importantly, some respondents acknowledge significant deficiencies within their business continuity preparations, while others report low levels of disruption management preparedness. The findings suggest that improvement to port risk management and disruption management capabilities is required before managers might effectively direct their attentions towards resilience enhancement.

Academically, the research provides a tentatively clearer understanding of the status of Australian port risk management and resilience, and an associated compendium of port risk management and resilience literature. Within a practitioner context, the research provides recommendations towards enhancing port risk management and resilience capabilities and contributes a theoretical basis for advancing management knowledge. Notional performance models are generated to provide potential means of assessing progress towards port risk management and resilience maturity.

Acknowledgements

I wish to thank my two supervisors, Associate Professor Stephen Cahoon and Associate Professor Benjamin Brooks for their assistance, patience and guidance in this research journey. From you both I learned much.

I am also grateful to the University of Tasmania for enabling me to participate in this higher degree research. I appreciated the many discussions on Campus with fellow research candidates, and our always stimulating interchange of ideas. Good fortune to you all, in your new careers.

Thank you also to the Australian port managers who generously contributed their knowledge and experiences towards this research, and to the staff of Ports Australia who promoted the research survey to their port management members.

I am indebted to my wonderful wife, Helen Justice, who supported and encouraged me throughout this lengthy endeavour.

Abbreviations and Acronyms

ACC	Australian Crime Commission
ACT	Australian Capital Territory
ADG	The Australian Dangerous Goods Code
AG	Australian Government
AIHW	Australian Institute of Health and Welfare
ALC	Australian Logistics Council
AMSA	Australian Maritime Safety Authority
ANFOmix	Ammonium-nitrate-fuel-oil mix
BITRE	Bureau of Infrastructure Transport and Regional Economics
BOM	Australian Bureau of Meteorology
CCTV	Closed-circuit television
CEO	Chief Executive Officer
COSO	Committee of Sponsoring Organizations of the Treadway Commission
CPA	Chartered Public Accountant
CRO	Chief Risk Officer
DFAT	Australian Department of Foreign Affairs and Trade
D&HG	Dangerous and hazardous goods
DoT WA	Department of Transport, Western Australia
DUKC	Dynamic Under Keel Clearance
ERM	Enterprise Risk Management
IA	Infrastructure Australia
IALA	International Association of Marine Aids to Navigation and Lighthouse Authorities
ICT	Information and communications technology
IRGC	International Risk Governance Council
ISO	The International Organization for Standardization
ISO/IEC	Joint technical committee of the International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC)
LNG	Liquefied natural gas
MTOFSA	Maritime Transport and Offshore Facilities Act (Australia)

NOAA	National Oceanic and Atmospheric Administration (United States)
NTRC	National Transport and Rail Commission
OEM	Western Australia Office of Emergency Management
PIANC	Permanent International Association of Navigation Congresses - World Association for Waterborne Transport Infrastructure
PPRR	Prevention, preparedness, response and recovery
PRQ	Primary Research Question
RDA	Regional Development Australia
RM^3	Risk management maturity model
SRQ	Secondary Research Question
SWOT	Strengths, weaknesses, opportunities and threats
TEMP	Tasmanian Emergency Management Plan
TISN	Trusted Information Sharing Network
TNT	Shipper TNT Express, a FedEx subsidiary
UHF	Ultra-high frequency
UNCTAD	United Nations Conference on Trade and Development
VAM	Vulnerability Assessment Model
VHF	Very high frequency radio
VIC	State of Victoria
VTS	Marine vessel traffic service
WA	State of Western Australia
WEF	World Economic Forum

Contents

Chapter 1: Introduction

> *Risk management helps the system prepare and plan for adverse events, whereas resilience management goes further by integrating the temporal capacity of a system to absorb and recover from adverse events, and then adapt (Linkov et al. 2014, p. 407).*

1.1. Research background

Risk management, in general, is a well-covered topic with centuries of evolution (Bernstein 1998). However, the 21st Century brings new forms of hazards and disruption that impact across industry sectors, geographic boundaries and supply chain systems, with potential for unexpected and unforeseen consequences (Fiksel *et al.* 2015; WEF 2018). Risk, according to the Australian Institute for Disaster Resilience (AIDR 2018, n.p.) is defined as:

> The likelihood that a hazard will happen, its magnitude and its consequences. It relates to the probability of external and internal threats (such as natural hazards…) occurring in combination with the existence of individual vulnerabilities.

From a logistics perspective, disruptions are regarded as '…unplanned and unanticipated events that disrupt the normal flow of goods and materials within a supply chain' (Craighead *et al*. 2007, 132). Types of disruption include adverse natural events, shipping accidents, technology and communications breakdowns, socio-political pressures, or deliberate harmful acts (Tang 2006a, 2006b; Waters 2011; Lam & Yip 2012). Innovative response and recovery techniques are increasingly required in responding to and recovering from new disruption causalities (Schiffino *et al*. 2017; WEF 2018). However, the impact of unexpected and unforeseen hazards is minimally addressed by the academic community including consideration of how port managers might respond to and treat disruptions that emerge from outside of their planned risk identification and treatment parameters. The primary objectives of this thesis are to gather clearer understandings of port managers' disruption experiences, how they

managed past emergency situations, their risk expectations for the future, and how resilience might enhance their emergency management and business continuity capabilities.

1.1.1. Port safety and safe ports

Burns (2015) describes the world's approximate 9,000 ports as strategic intermodal transhipment nodes, acting as crucial links between land and waterborne transportation to enable the two-way transfer of more than 10.6 billion tonnes of international maritime trade (UNCTAD 2017). Ports are meant to provide safe havens for ships at the end of each voyage, along with the necessary facilities for loading and unloading cargoes (Burns 2015). A 'haven' is described by the Oxford Dictionary as a port or harbour that provides safety and shelter for ships. The provision of safe ports for ships is a crucial attribute within both risk management and commercial contexts, to the extent that shipowners and ship charterers enter into arrangements for the nomination of a safe port. A safe port has been characterised by a long-standing legal ruling that:

> A port will not be safe unless, in the relevant period of time, the particular ship can reach it, use it and return from it without, in the absence of some abnormal occurrence, being exposed to danger which cannot be avoided by good navigation and seamanship, it would probably meet all circumstances as a broad statement of the law[1].

Managing port risks against the threat of known types of disruption has long challenged those responsible for port safety. During the fifth and fourth centuries BC, high stone walls were constructed around the Athenian ports of Piraeus and Phalerum to protect wharves, storehouses, port assets, and road corridors against Persian

[1] Safe Ports: *Leeds Shipping Company Ltd v Société Francaise Bunge (The Eastern City)* [1957] 2 Lloyd's Rep 153, 158

attack (Burns 2015). The contemporary port risk environment requires barriers of far different types, with the emergence of unpredictable and unforeseen hazards lending new dimensions of uncertainty to port operations and networked stakeholders (Yang *et al*. 2014; Lam & Lassa 2017; Tucci 2017; WEF 2018). Within this research, uncertainty is regarded as a port manager's limited knowledge about risk-related events, particularly when information concerning the risk environment might be unreliable or imprecise (Walker, Lempert, & Kwakkel 2013; Brooks *et al.* 2018).

Questions about what determines a safe port and the charter party implications of this 'safe port' clause attract a large and growing body of literature (Chong 1992; Astle 1996; Parkes 1998; Singh 2008; McKinnon 2009; Mandaraka-Sheppard 2014**;** Todd 2015; Schoenbaum 2016; Girvin 2017). While many academic and legal researchers study what constitutes safe port characteristics and port safety outcomes for ship and cargo operations, few studies focus on *how* the functional risk management aspects of a safe port might be achieved. Or, more specific to this thesis, how Australian port managers manage the risks of high consequence hazards and uncertainties that threaten their ports. This research problem is regarded as a worthy area for research, with Van der Vegt *et al.* (2015, p. 2) inviting '…management scholars to take up the "grand challenge" of studying the role and functioning of organizations during adverse natural or social events'.

1.1.2. Potential contributions to the knowledge

This study aims to broaden theoretical and empirical risk management knowledge by investigating Australian port management effectiveness in managing risks, deep uncertainties and consequences arising from unplanned and unanticipated disruptions. The study explores how risk management effectiveness might be enhanced through operationalising resilience theory into practice against the impact and consequences of disruptive events and identifies some change management factors that either promote or impede resilience initiatives at Australian ports. Organisational competencies in managing a challenging risk environment while simultaneously providing reliable and effective services are attributes related to high

reliability organisations, or in relation to ports, to high reliability port networks (Wood, Dannatt & Marshall 2006; Bethod *et al.* 2016). High reliability theory is associated with resilience theory within the literature, whereby high reliability organisations are assessed in part by their commitment to resilience (Wood, Dannatt & Marshall 2006; Weick & Sutcliffe 2015; Berthod *et al.* 2017).

Four decades ago, researchers were setting their research agendas to establish whether and how, for example, computer technology might be used to assist in port management and arguing that more attention should be directed towards low risk/high consequence port facility hazards (Price, Friedheim & Ross 1983). Port managers today have considerably broader risk and vulnerability issues than did their 1980's predecessors. Port business processes depend upon the availability and reliability of externally provided crucial goods and services, inclusive of the technology inputs that underpin transport, logistics and port operations effectiveness (Van den Berghe 2015; Ferretti & Schiavone 2016; Heilig & Voß 2017a, 2017b). Port dependencies upon external stakeholders suggest that port risk management and business continuity processes can no longer be studied in isolation – by association, crucial goods and services supplier vulnerabilities become port vulnerabilities. Contemporary risk management researchers provide important information about these networked interrelationships and dependencies between the port and its crucial hinterland goods and services suppliers (Wakeman 2013; John *et al.* 2015; Wei, Chen & Rose 2017). This research attempts to add to the knowledge by leveraging from these studies.

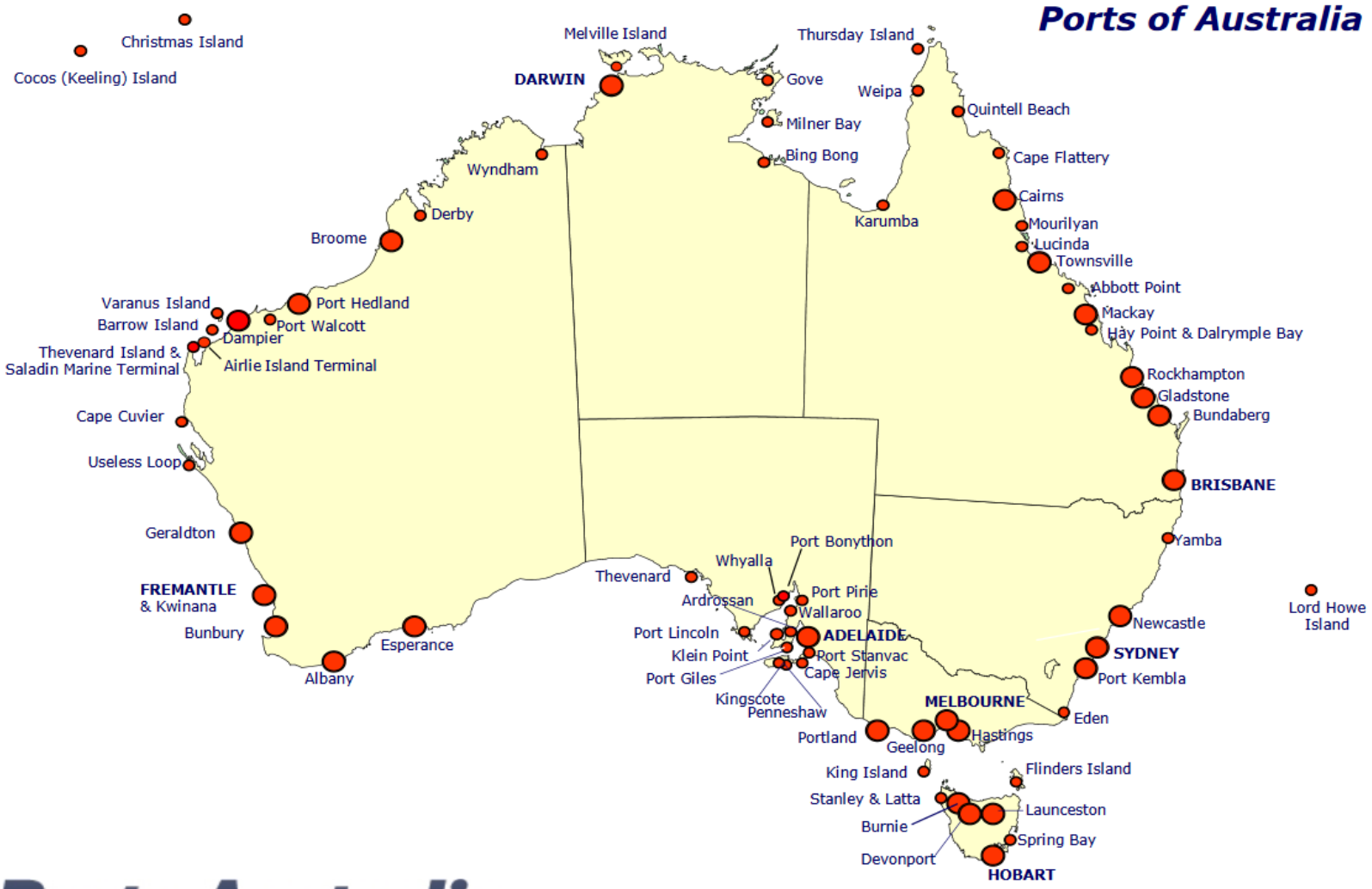
1.2. Research context and importance of Australian port operations

Ports conduct their complex intermodal shipping operations within a fast-moving, dynamic and tumultuous risk environment in which business-as-usual normality might quickly be replaced by emergency conditions. Rapid transition to emergency conditions is a characteristic, for example, of cyber-attacks against critical port operating and administration systems (Clark & Hakim 2017; Tucci 2017). Increasingly, Australian ports as critical infrastructure elements must optimise their risk

management capabilities and emergency preparedness for planning, preventing, responding, recovering and learning from disruptions (Zio 2016). This is recognised by Australian government initiatives towards critical infrastructure protection, which encourage ports and other Australian critical infrastructure operators to strengthen their resilience capabilities and capacities (AG 2015; TISN 2015).

During 2017, over 80% by volume (more than ten billion tonnes) of the world's raw materials and manufactured goods passed through global ports. Seaborne trade growth is influenced in part by Australian trading partners such as China, Japan, the US and South Korea (Branch & Stopford 2013; DFAT 2017; UNCTAD 2017). Within a critical infrastructure context, ports are essential to the conduct of international business and the continued operations of global supply chains, the security of the Australian economy, and to the employment and economies of port centric regional communities and their industries (AG 2015; Burns 2015; Cavusgil *et al.* 2015; IA 2016). The publication *Guide to Port Entry* (Witherby 2018) lists 86 major Australian commercial ports and terminals, of which 70 are of appreciable value to global trade (Ports 2017). A study of one such port (Nicolaou, Buckland & Hammond 2017) estimates that in 2015-16 the Port of Port Hedland in Australia's north west generated AU$18.5 billion in direct economic output for the Western Australian State economy, AU$30 billion to the Australian economy, and supported 86,240 full time jobs.

Australian ports are managed, overseen and regulated by 27 port authorities and State government transportation departments (Ports 2017) and these management entities are responsible for matters of port safety and risk management under national and State Acts, regulations and industry codes of practice (AUSTLII Data Base 2018). A map of Australian ports is shown in Figure 1-1 (Ports 2017), which also indicates the boundaries of the various Australian States. Australian ports come under the jurisdiction of State governments. Most ports are administered by port authorities acting as corporatised statutory authorities, however a perception exists that these port management organisations are not far removed from political and government interference (Chen & Everett 2014).



Ports Australia

Figure 1-1: Australia and its ports (Ports 2017).

According to Chen and Everett the continuing political oversight and control over Australian ports impedes port managers from acting quickly and flexibly to dynamic changes in their working environment. The literature provides little further evidence of how this political constraint might work to impede port risk management processes and procedures, or to compound an already complex risk environment.

Australia is a large island continent that geographically encompasses diverse mineral and rural resources that shape the creation and growth of its ports, and multiple climate zones with individual climatic influences upon port operations (Parker *et al.* 2009). Australia's mainland and ocean territories are segmented into 55 development zones termed as regions, and these are shown in Figure 1-2 (RDA 2018). Some Australian geographic regions are larger than smaller European nations, and a recent port reform trend is for Australian port authorities to manage all ports within their geographic region, to form a system of networked ports (DoT-WA 2017).

Conceptually, the broader academic literature tends to associate port regions and regionalisation with the relationships between a port and its hinterland stakeholders, coupled with port effects upon the regional economy and its industrial growth (Notteboom & Rodrigue 2005; Notteboom, Ducruet & De Langen 2009; Wilmsmeier, Monios & Rodrigue 2015). Throughout this research, however, reference to Australian regions indicates non-capital city zones formed by geographical, climatological and economic segmentation of national land areas (Parker *et al.* 2009; Eversole 2016). Regions mentioned in other literature cited within this research generally refer to port-centric hinterlands. Australian port managers confront varying types of regional risks, where for example port climate change adaption needs depend upon geographical location (Parker *et al.* 2009; Hodgkinson, Hobday & Pinkard 2014). Also, regional ports might be located more than 1,000 kilometres distant from their State capital city and its central pool of emergency response services and resources (AG 2011, 2018).

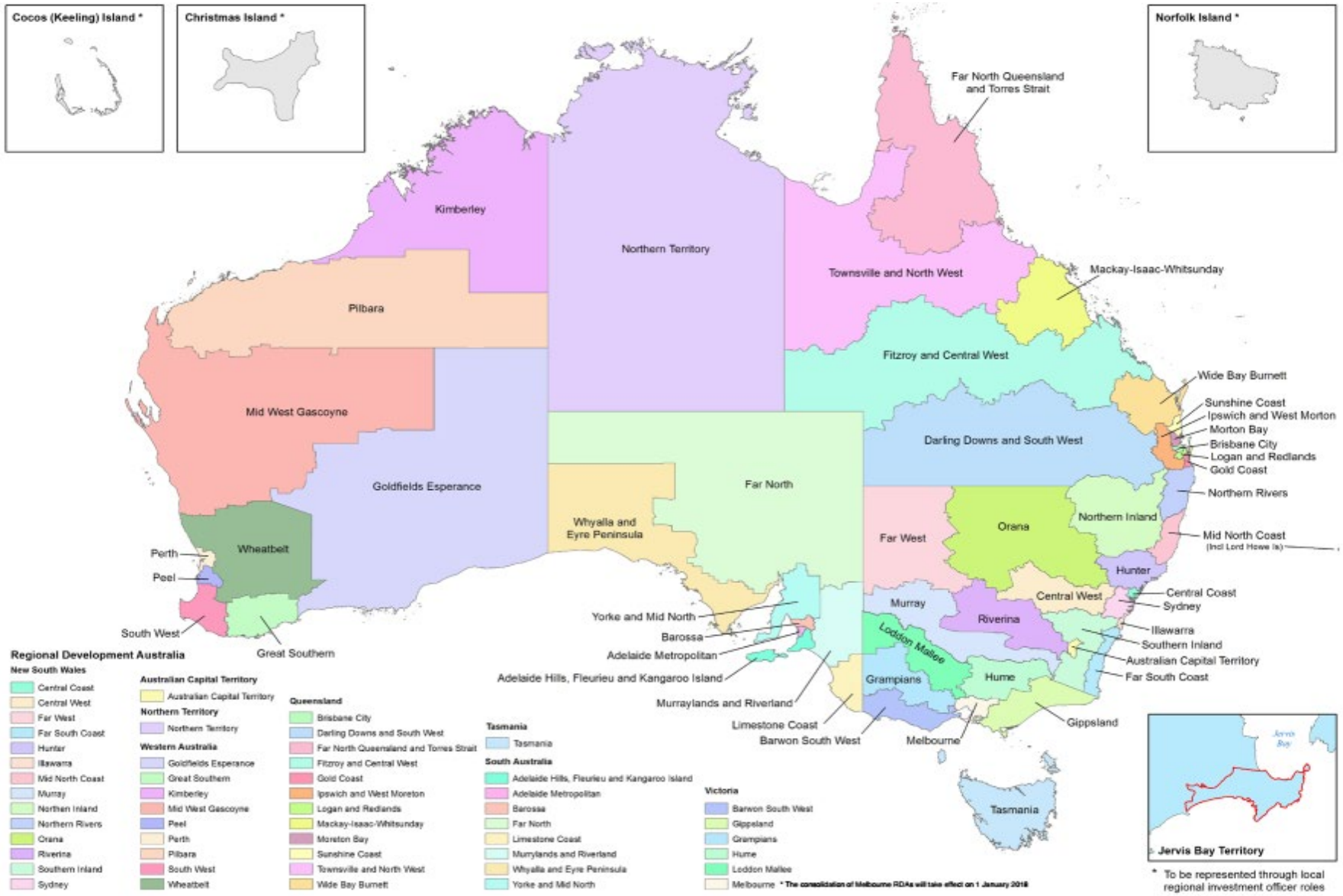


Figure 1-2: Australian regions (RDA 2018).

Geographical isolation from capital city external support requires Australian port managers to develop competent internal governance and capabilities for managing disruptive circumstances within an incident control function (AIIMS 2017; Wakeman *et al*. 2017). Within a research context, little is known of Australian port managers' capabilities for dealing locally with potential new hazards, their capabilities for emergency response and disaster recovery, or what resilience measures they might employ (Trucco & Petrenj 2017; Wei, Chen & Rose 2017). Recognition of that research gap has led to this investigation.

1.3. Port hazards, risk management and organisational resilience

Research discussion is immature about Australian port hazards, risk management and resilience capabilities, despite the potential harm that new and emerging risks might pose to ports, and Australian government concerns for critical infrastructure protection. These knowledge gap and risk environment pressures lend both importance and timeliness to this study. Hazards originate both within and external to port operations, and those potentially within port managers' abilities to control give rise to human, technological and infrastructure risks (Thai & Chen 2011; MacKenzie 2012). Hazards beyond port managers' abilities to control might result in unforeseen or unexpected disruption onsets and/or consequences, for example adverse natural events, shipping accidents, technology and communications breakdowns, socio-political pressures, or deliberate harmful acts (Tang 2006a, 2006b; Waters 2011; Lam & Yip 2012). Difficulties in establishing risk controls due to hazard uncertainties and unknowns might influence managers to develop alternative and non-traditional capacities for coping and responding to disruptions, and these processes and procedures are germane to systemic resilience (Welsh 2014; Coaffee & Clarke 2016).

For Australian ports, uncertainty might arise from management inabilities to predict or foresee unknown elements of risk, creating what is termed 'wicked problems' (Smithson 2010; Gharehgozli *et al.* 2017). These wicked problem risks include adverse natural events of increasing severity (WEF 2018) with, for example, fewer Australian

tropical cyclones predicted but of greater intensity, stronger wind speeds and higher rainfall (BOM 2018). Conventional risk management techniques focus on *known* and *quantifiable* risks (ISO 31000:2018), however risk management to treat uncertain and unexpected adverse events involves a complex interrelationship between plans, processes and strategies to identify, assess, prepare, respond, manage and recover from disruptions (Srikanth & Venkataraman 2013; Bichou, Bell & Evans 2014; Booth 2015; Hopkin 2017; Lam & Lassa 2017; Haimes 2018). Further, treating 'wicked problems' requires management to cope with disruption complexity and diversity while possessing only fragmented and incomplete knowledge (Head & Alford 2015). Head and Alford suggest that there is no single or best solution to identifying and managing ambiguous disruptions and their potential consequences, rather an effective response to such risks might be reactive, adaptive, collaborative, coordinated, and managed within leadership that reflects these qualities. Because the port risk environment is characterised by unknowns, uncertainties, unexpectedness and unpredictability (Chandler & Coaffee 2017; Haimes 2018), then this research assumes that contemporary port risk management requires more adaptive and innovative capabilities for managing risks than those enabled by conventional means. This assumption is supported from within the resilience-oriented literature (Gibson & Tarrant 2010; Chandler 2014; John *et al*. 2016).

The literature provides a confusing range and imprecision of resilience definitions. Moteff (2012, p. 2) is one researcher who expresses a frustration with the definitional imprecision by stating: 'there are almost as many definitions of resilience as there are people defining it'. The International Standards security and resilience standard (ISO 22316: 2017, p. 1) for example, provides resilience knowledge and guidance that port managers can access, and defines organisational resilience as:

> The ability of an organization to absorb and adapt in a changing environment to enable it to deliver its objectives and to survive and prosper. More resilient organizations can anticipate and respond to threats and opportunities, arising from sudden or gradual changes in their internal and external context.

> Enhancing resilience can be a strategic organizational goal and is the outcome of good business practice and effectively managing risk.

This resilience standard is recent, and the time lag between its publication and when any widespread manifestation of its benefits will appear in the port workplace is yet to be tested. Two other standards associated with port resilience are ISO 31000:2018 on Risk Management – Principles and Guidelines, and ISO 22301: 2012 on Business Continuity. Risk management and business continuity are associated with planning and preparation phases of disruption management capabilities, whereas the manifestation of resilience is more likely to appear *during* a disruption, or as described by Booth (2015), resilience refers to the enablement of further coping with abilities during crisis management.

1.4. The research problem

At a time of emerging and unforeseen hazards and uncertainties that threaten global critical infrastructure, this research investigates Australian port management abilities to manage high consequence disruptions from known and unknown causalities. By reconceptualising the port as a regional system of networked logistics and transportation clusters and operators, the research aims to provide new and deeper insights into port risk management capabilities, reliability, and resilience. The research problem is based upon how Australian ports manage risks and consequences arising from low probability/high consequence hazards, and the extent that their safety performance and freight task continuity relies upon resilience as a defence-in-depth against unexpected and unforeseen disruptive events.

Topicality and importance of these resilience aspects arise from Australian government initiatives to strengthen Australian critical infrastructure resilience levels (O'Donnell 2013; AG 2015; IA 2016). Further impetus arose in 2017 when disastrous cyber-attacks shut down components of the Port of Rotterdam, Maersk shipping, TNT, global banks and critical infrastructure including power stations for several days (Roth & Nakashima 2017). More generally, academics and practitioners are presently

engaged in quantifying and redefining resilience as practised within large and complex organisations (Hosseini, Barker & Ramirez-Marquez 2016). Whereas academia appears to be well advanced in exploring transportation and logistics resilience (see for example Mattsson & Jenelius 2015; Pitilakis *et al.* 2016; Shaw, Grainger & Achuthan 2017), few researchers address Australian port practitioners' risk management and resilience capabilities. Instead, Australian port-centric resilience studies tend to take a climate change perspective (McEvoy & Mullett 2013; Cahoon *et al*. 2015; Yang *et al.* 2015). This explains why Australian port resilience research is small when compared with the volume of European and US port resilience studies (Rose & Wei 2013; Loh & Thai 2014; Pant *et al*. 2014; Trepte & Rice 2014; John *et al*. 2016; Shaw, Grainger & Achuthan 2017; Vonck, Notteboom & Dooms 2017; Wei, Chen & Rose 2017).

The intention of this thesis is to address gaps in the knowledge by conducting empirical research that:

a) identifies Australian port characteristics and vulnerabilities to operational risks;
b) identifies hazards that potentially threaten port business continuity;
c) assesses port manager capabilities for responding to and managing these hazards;
d) provides a clearer understanding of the terminology and practical employment of port resilience;
e) explores what might enable or constrain Australian port resilience practices; and,
f) investigates how ports might operationalise resilience to best manage/mitigate risks and unknown unknowns arising from emerging categories of low probability/high consequence disruptive events.

1.5. Research questions

The primary research interest is to gain a clearer understanding of how effectively Australian port managers manage risk, and cope with disruptions in crisis management and business continuity endeavours. Empirical components of this research set out to determine what risk and resilience capabilities and capacities are evidenced by managerial self-reports. Research validity rests upon assumptions that the survey respondents as port senior decision-makers are attentive and knowledgeable about their risk management roles and responsibilities, and knowledgeable about resilience competencies. Accordingly, this thesis investigates the underlying risk management concepts and practices that might result in safe port outcomes for Australian intermodal shipping operations, and therefore the primary research question (PRQ) is:

> How does the port manage risks and consequences arising from low probability/high consequence disruptions?

To investigate the PRQ in finer detail, three secondary research questions (SRQs) were developed, as follow:

> SRQ1: How do ports currently manage risks and unknown unknowns arising from disruptive events?
>
> SRQ2: What do ports need to change in their practices to become more resilient? and
>
> SRQ3: How might ports operationalise resilience to best manage/overcome risks and unknown unknowns arising from disruptive events?

1.6. Significance of the study

Although few studies address Australian port risk management and resilience, Australian government initiatives for critical infrastructure protection are strong motivation towards gaining a clearer understanding of port emergency management capabilities and processes, crisis management effectiveness, and resilience (AG 2011, 2015, 2017; IA 2016; TISN 2016). This study is intended for a potential audience of

academics, practitioners and regulatory authorities, with the objective of broadening theoretical and empirical risk management knowledge. Potential contributions include:

a) the use of Dynamic Capabilities theory in conjunction with systems and resilience theories, to explore how Australian ports might operationalise resilience to competitive advantage - an innovative and pragmatic approach that potentially provides a new methodology for gaining richer, deeper and more explanatory port management findings;
b) compilation of an extensive literature review related to the generic port risk management environment, which may serve as a research basis for other researchers within the field of critical infrastructure protection, as well as an informative guide for practitioners;
c) gathering information on new and emerging risks, and increasingly severe existing risks;
d) an investigation of port manager attitudes, behaviour and competencies in relation to risk management and operationalising resilience;
e) assessment of Australian port risk management effectiveness;
f) reconceptualising Australian port dependencies upon, and vulnerabilities arising from, crucial goods and services supply from land and sea;
g) establishing sufficiently valid macro-findings to be applicable in other fields of transportation research; and
h) providing knowledge that may be useful in assisting practitioners to expand their professional knowledge and awareness, and in enhancing their port preparedness towards future risks.

1.7. Thesis organisation

Figure 1-3 provides a graphical presentation of the Thesis structure to show the chapter interdependencies. The introductory chapter broadly explains the underlying circumstances leading to the research problem and provide a rationale for why the study is important. The literature and empirical research germane to the problem

being studied is summarised, and a logic framework constructed towards clarifying the research questions and aim of the study. The problem statement is explained, and the purpose of the study clarified. Chapter 1 also outlines the function of each succeeding chapter in developing the framework and focus of the thesis. Chapter 2 identifies and evaluates the characteristics and importance of Australian ports and port management. These characteristics and port managers' networked interrelationships and interdependencies with stakeholders render the port vulnerable to diverse hazards, which are discussed in Chapter 3.

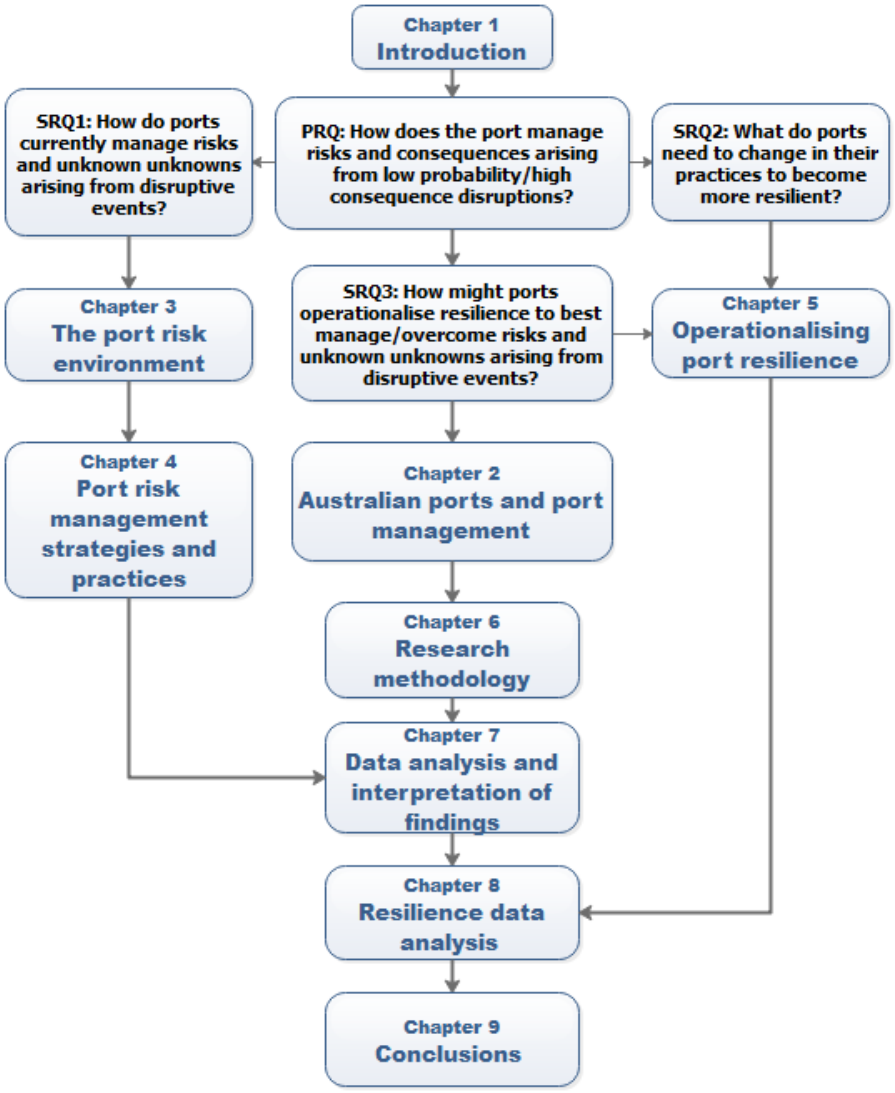


Figure 1-3: Thesis chapter outline (Author).

Port risk management is investigated in Chapter 4, from top-down and bottom-up management perspectives. Chapter 5 compiles a port resilience framework to provide a clearer understanding of resilience within a port operations context. Further, the chapter provides a conceptual basis against which port conditions conducive to strengthening resilience might be measured, Chapter 5 proposes a notional resilience maturity measurement model based on the conceptual model provided by Gibson and Tarrant (2010).

After gathering this information from existing theory, the thesis flows on to research methodology (Chapter 6), which explains the use of web-based, structured quantitative, and semi-structured qualitative survey questions in generating data to more completely answer the research questions. Chapter 6 presents the scientific methodology and the underlying logic in understanding the exploratory research problem. Chapter 7, the risk management data analysis and findings chapter, reviews the problem and associated issues, and is followed by Chapter 8 which assesses the challenging issue of how port managers might transform resilience theory into practice. Chapter 9 provides the thesis conclusions, and summarises the body of work inclusive of the literature review and the empirical research. Limitations of the study are described, and opportunities or possibilities for further research are suggested.

Chapter 2: Australian ports and port management

2.1. Introduction

Chapter 1 provided a brief overview of Australian ports' immense contributions to the national economy and towards the effectiveness of global commerce. Prolonged interruptions to port business continuity carry significant potential for widespread financial losses, plus adverse implications for supply chains and industries relying on just-in-time deliveries of goods and materials by sea. Port managers have heavy responsibilities in maintaining continuity of their intermodal operations, beginning with clear understandings of where and how their ports become vulnerable to a dynamic and uncertain risk environment. The aim of Chapter 2 is to contribute knowledge to this area of research by examining Australian port roles, characteristics, capabilities, relationships and crucial enabling requirements for maintaining the two-way flow of global trade. A clearer understanding of what constitutes a port and its nationally important intermodal operations is integral to subsequent chapters that examine the port risk environment and its hazard uncertainties, and how port managers might plan for, respond to, manage, and then recover from the impacts and consequences of actualised port hazards. Chapter 2 begins this process by discussing Australia's major ports and port authorities within their regional, national and global contexts.

2.2. Australian ports and risk management functions

In 2015-16, Australian ports enabled exports of 1.446 billion tonnes and imports of 150 million tonnes, representing AU$420B in two-way global trade (BITRE 2017). Australia's ports handle approximately 15% by weight of global seaborne trade and accordingly, any prolonged disruption to these ports' operations threatens multiple nations' economies and related supply chains' effectiveness. The scale and economic value of this seaborne trade illustrates the importance of Australian port managers' risk management effectiveness. Effective risk management capabilities are the delegated operational and strategic responsibilities of port managers, whose port

authorities are tasked by governments with maritime safety, security and crisis management (Berle, Asbjørnslett & Rice 2011a). The peak body for Australian ports, port authorities and associated public and private entities is Ports Australia, and their map (Figure 2-1) is adapted to show the location of Australian ports, port authorities and State government departments with regulatory responsibilities for ports.

Australian ports are managed by six State government departments, and twenty-one port authorities operating as corporatised public facilities. Decadal port reform processes and asset sales have seen some ports privatised in the form of long leasehold arrangements, but these privately-operated ports remain overseen by port authorities in a regulatory role (Everett 2007; De Langen & Haij 2014; Chen, Pateman & Sakalayen 2017). The Australian port privatisation process is prone to socio-political tensions, where the port authority remains responsible for privatised port operational safety and security, providing emergency response and recovery services, and regulating the two-way transit of dangerous and hazardous goods (Chen, Pateman & Sakalayen 2017). It is not known, post these privatisation and port reform processes, how well-resourced Australian port authorities might be in facilitating their risk management roles and functions.

2.2.1. Port failure modes and vulnerabilities

Australian ports have evolved in multiple ways depending upon their locations, purposes, trade patterns and demand, port ownership, ship sizes, national defence influences, and regional industry requirements (Alderton & Saieva 2013; Burns 2015; Sakalayen, Chen & Cahoon 2017). Supply chain managers might view ports as costly but essential intermodal transit points for their cargoes (Song & Panayides 2008); the local community might regard the port as a source of employment and business opportunities (Notteboom 2010) or even a source of environmental annoyance; while governments might view the port as an instrument for regional development and economic gain (Bottasso *et al*. 2014; Sakalayen, Chen & Cahoon 2017).

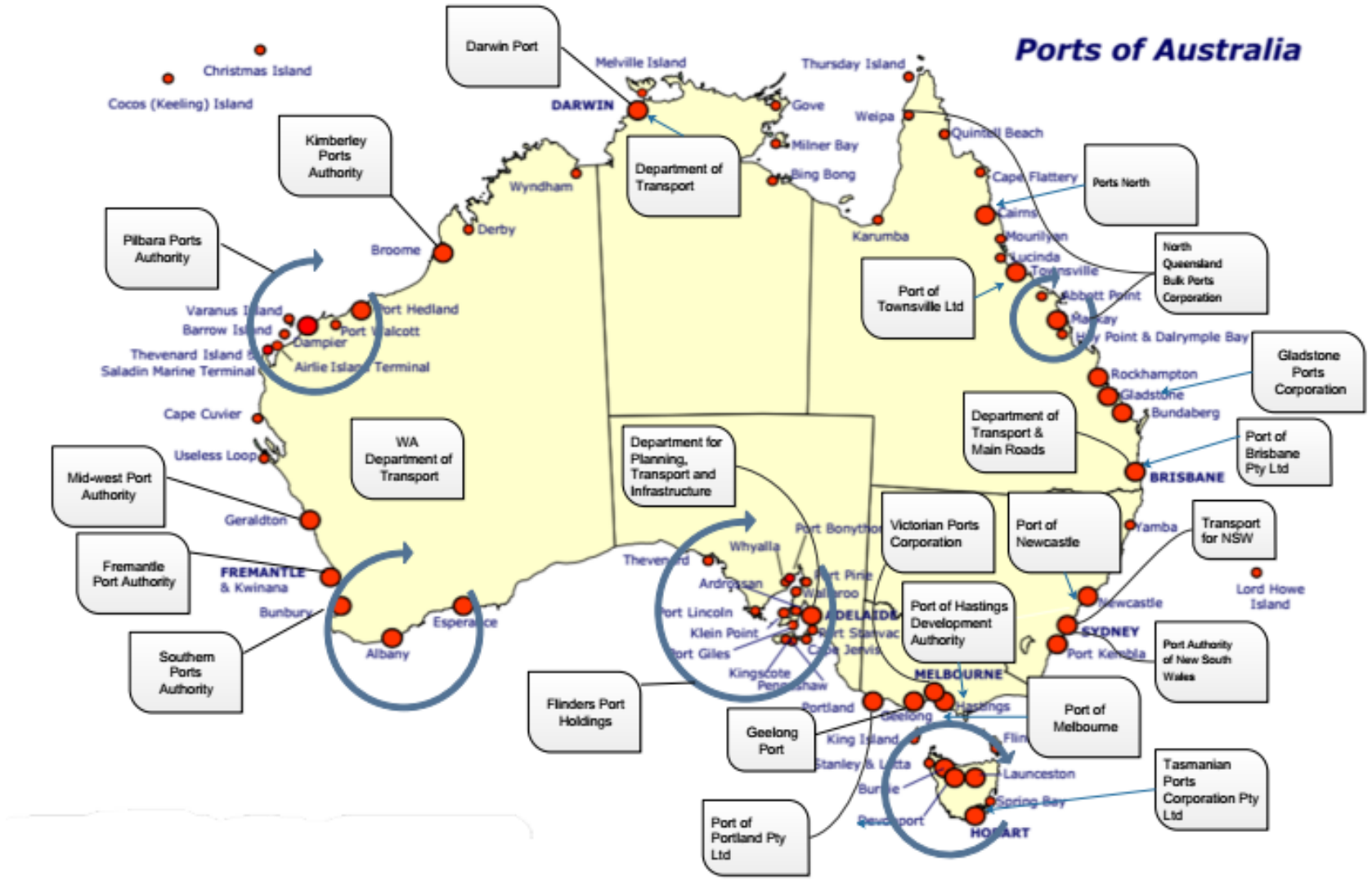


Figure 2-1: Major ports, port authorities and port-related State government departments (Adapted from Ports Australia 2017).

The primary purposes and operations of ports and port authorities are summarised by Burns (2015):

> Seaports are principally designed to provide shelter to oceangoing or inland ships, while effectively managing numerous dissimilar activities, human force, materials, and financial resources. Port authorities are in charge of harboring and securing ships, while ensuring smooth operations throughout ships' anchorage, pilotage, berthing/unberthing, lightering, mooring/unmooring, loading/unloading operations (2015, pp 1-2).

Ports evolve in individual ways because of their dissimilar activities and characteristics. Their evolution, management and governance are also shaped by whichever ownership and structural model applies to their port. The World Bank (PPIAF 2016) describes varying types of port management models, each of which demonstrates differing levels of port authority management involvement:

a) fully port authority operated facilities (service port);
b) tool port models wherein the port authority is vested by the State government with the port land and sea holdings, and leases out operations to services companies;
c) a landlord port model where the port authority leases sites to operators who then provide requisite infrastructure and superstructure; or
d) a fully privatised port for which the port authority is responsible for regulatory and administrative roles and functions.

Port management roles, responsibilities, and levels of authority are influenced by the nature of port ownership, its structure and organisation (Burns 2015). These influences are rarely discussed within the context of managing operational risks. Burns (2015) argues that ports owned by governments and operated by port authorities are less vulnerable to risk consequences, one reason being that the government owner is a source of last resort for financial subsidies, grants and cash injections. A port managed by a government business agency might also tend towards low-risk, steady growth management strategies in line with what is described as a port authority mindset with bureaucratic tendencies (Everett 2007;

Chen & Everett 2014). Alternatively, a fully privatised port might be more vulnerable to risk consequences, and in the case of a foreign port operator, an Australian port may be exposed to fresh sources of socio-political risk. Yet unknown are potential strategic and management oversight risks (if any) arising from foreign investment in Australian ports and port operations, for example the Northern Territory Government leasing of Port of Darwin facilities to a Chinese-owned company for 99 years (Barnes *et al.* 2015).

In general, little is known about how Australian port authorities might manage and respond to uncertainties arising from port infrastructure, facilities and operations increasingly being delivered into private sector control. Chen, Pateman and Sakalayen (2016) argue that when Australian port corporatisation and privatisation initiatives occur, then the port authority or relevant State government departments remain responsible for port regulatory governance and emergency management roles but lose some influence over how port business operations are conducted. This suggests that private sector port risk management interests and directions might not necessarily coincide with those of the port authority. Since 2010, an objective of Australian port reform processes was to make port management more efficient (Chen, Pateman & Sakalayen 2016). Various State port reform processes result in port authorities experiencing reduced control over port operations, while retaining compliance responsibilities for regulatory governance and emergency management, sometimes under bureaucratic and political interference (Chen & Everett 2014; Chen, Pateman & Sakalayen 2016). How these constraining factors might affect port risk management and resilience effectiveness remains to be explored.

Port operational capabilities are shaped by its physical attributes (geography, infrastructure, superstructure and assets), human resources (port employees and contractors and external goods and services providers), management systems (plans, procedures and capabilities), and, the use of technology (information, communications, logistics, management systems, hardware and software) (Burns 2015; John *et al*. 2015; Price & Hashemi 2016; Bichou 2018). A list of the port's crucial enabling requirements is sourced from the literature and shown in Table 2-

1 (Bridges 2004; Rodrigue, Comtois & Slack 2009; Lansdale 2012; Tsinker 2014; Price & Hashemi 2016; Bichou 2018).

Port operational capabilities	**Crucial enabling requirements**
Safe ship navigation	Berthing pockets and turning areas, breakwater/s, channels, charts, Harbourmaster oversight and directions, navaids, navigational safety system, pilotage, pilot launch &/or helicopter, towage, VTS.
Infrastructure	Dredged channels and seabed areas, dry docks and slipways, green areas, land, laydown and storage areas, paving, pipeline and conveyor corridors, road and rail connectivity, wharves.
Superstructure and equipment	Amenity blocks, boat ramps, cargo handling and ship/shore transfer equipment, cargo transport vehicles, cathodic protection system, conveyors, DGPS and RFID tracking systems, dry bulk silos, electrical distribution and substations, emergency power and lighting, fencing, fenders and pontoons, firefighting system, fixed and mobile cranes, footpaths, fuel tank farm, hydro-meteorological monitoring system, ICT/intranet system, landside navigational markers and leads, lighting, marinas, marshalling yards, motor vehicles, offices and meeting rooms, oil and chemical spill equipment, pipelines, potable water system, radio and radar installations, recreational boating areas, road/rail traffic management system, roads, security system, sewage system, ship/boat lifter, small craft/launches, storm water system, surveillance system, terminal operating systems, terminals, tug pens, VTS centre, warehouses, water and fuel lighters, weigh bridges, workshop and tools.
External services and supply	Agents, asset and machinery repair, aviation (fixed wing and rotary), banking and finance, bunkering, catering, chandleries, cleaning, consignees, customs, distribution, diving and underwater maintenance/repairs, dredging, electricity, fabrication, food, freezing and chilling storage, fuel, hospitality and housing, ICT, immigration services, insurance, investment, ISP, linesmen, livestock holding yards, logistics and transportations services, maintenance, manufacturing, medical and health, pilots, police and emergency services, port labour, providores, public transport, quarantine, shippers, road and rail transportation, stevedores, training, tug crews, waste removal, waste water, water treatment.

Table 2-1: Port capabilities and crucial enabling requirements (Adapted from the literature).

A primary objective of port operational management is to maintain a reliable two-way flow of freight and passengers through the port, while ensuring safe, secure and effective ship navigation, the safe and effective transfer of cargo from one means of transportation to another, and safe movement of passengers between ship and shore (Lansdale 2012; Stopford 2013; Burns 2015). At each stage of a ship visit the port is exposed to the risks of accidents with potentially severe consequences including loss of life, environmental pollution, and widespread damage to the ship, other vessels and to port infrastructure (Hsu 2015).

The ship visit commences upon arrival at port, whereupon the Master is directed by the VTS officer (on behalf of the Harbourmaster) to proceed either to an anchorage area, normally within port limits, or to a pilot boarding position from which the ship is navigated to the requisite berth in port (IALA 2016; Lansdale 2012). Port navigational services are assigned to the vessel which makes its way to the designated berth. Once the ship is secured to the berth and requisite ship/shore safety checks are complete, then the cargo loading or unloading operations commence. Cargo transfer equipment varies according to the type of cargo, and at a small port there might be only one wharf with multiple cargo handling capabilities and diverse equipment (Burns 2015; World Bank 2016). At larger ports multiple terminals specialise in single types of cargo handling, for example either dry or liquid bulk handling, break bulk or containers. When the cargo transfer to or from the ship is complete, then the ship departs the port and the port prepares for the next shipping operation.

For managers to maintain the continuity of their port business, shipping and cargo operations should be protected both from foreseeable risks of knowable causes, and from low frequency/high impact disruptions whose causes may be yet unknown and unpredictable (Berle, Asbjørnslett & Rice 2011a). Port managers may not know or be able to predict the onset of what Gharehgozli *et al.* (2017) describe as 'wicked problems'. However, these managers could identify and assess wicked problem consequences, whose impact upon port vulnerabilities would be sufficient to create failure modes and to halt shipping and cargo throughput **(**Berle, Rice & Asbjørnslett 2011a, 2011b). This process is termed a vulnerability

assessment, which leads to the understanding of what key functions and capabilities constitute weak links within port operations, what resources should be provided to protect these failure modes from harm, and what alternative or duplicated resources might enable port business to continue or expeditiously resume functionality following a disruptive event (Schnaubelt, Larson & Boyer 2014).

Green (2008a) defines vulnerability as exposure to a hazard, whereby the level of organisational vulnerability might vary inversely to organisational preparedness and mitigation. Vulnerability is arguably a dynamic risk factor when the organisation adjusts its functioning to manage expected and unexpected conditions, by means of changes in operational practices, training program effectiveness, environmental conditions, and the extent of organisational hazard mindfulness (Green 2008b; Weick & Sutcliffe 2015; Burnard, Bhamra & Tsinopoulos 2018). Port vulnerabilities to hazards vary from port to port due to the individual port characteristics as previously described, and because a port's exposure to adverse natural events depends to some extent upon its geographic location. For example, a port in the southern half of Australia is minimally vulnerable to cyclones, because cyclones degrade into low pressure weather patterns as they move into cooler climate zones (BOM 2018; Bartlett & Singh 2018).

2.2.2. Linking risk management with vulnerability assessments

A determinant of port risk includes the vulnerability of all crucial requirements at risk (Cardona *et al.* 2012; Zio 2016). Within a port vulnerability assessment, each of the crucial operational capabilities listed at Table 2-1 constitutes a point of vulnerability that port managers should address (Hsieh, Tai & Lee 2014; Schnaubelt, Larson & Boyer 2014; Pitilakis *et al.* 2016). Potentially each port has multiple and complex 'crucial enabling requirements' and resultant vulnerabilities requiring conventional risk management treatment, coupled with ongoing vulnerability assessments, controls and mitigation (Berle, Rice & Asbjørnslett 2011a). Further, because Table 2-1 reveals that port business also relies upon crucial external services and supply for its business continuity, then a need arises

for collaborative as well as individual risk and vulnerability treatments. Friday *et al.* (2018) identify key components of collaborative risk management as information sharing, standardised risk management procedures, collaborative and coordinated decision-making, the sharing of risks and beneficial outcomes, with enactment through aligned risk management processes and performance systems. Little is known about the extent of collaborative risk management implementation across Australian port stakeholders.

Vulnerability is described by Gallopin (2006) as a system's potential towards a relatively permanent and profound transformation to another state if a sufficiently strong disruption arises from either internal or external origins. The degree of change is relative to the system's exposure, sensitivity, and adaptive capacity to the disruption (Gallopin 2006). Vulnerability, according to Haimes (2016, p. 493) represents the exposure to harm of a system's 'physical, technical, organisation and cultural' states. In the case of the port, key operational vulnerabilities affecting business continuity include the safety of navigation in port waters, safeguarding the port's land and sea infrastructure and superstructure, and ensuring the supply of crucial external goods and services (Alderton 2013; Bichou, Bell & Evans 2014; Burns 2015; John *et al.* 2015; Price & Hashemi 2016). Exposure is described as the extent and time that the system is influenced by the disruptive event, sensitivity as the potential degree by which the system might alter in response to the perturbation, and adaptive capacity as the ability to adjust, absorb and turn to advantage the harmful influences of the perturbation (Gallopin 2006).

The linkage between port vulnerabilities and risk management becomes an important consideration for port managers, not only because of the value of trade and port business, but because ports represent significant investments at risk to hazards. Australian LNG ports and terminals (for example Wheatstone, Gorgon, Dampier, Darwin and Gladstone) are expensive to construct. A small port might cost A$15 billion, whereas Australia's Gorgon facility (the world's most expensive LNG port project) cost A$52 billion (Songhurst 2014). A container terminal such as Australia's Webb Dock facility is estimated to cost A$1.6 billion and retrofitting of

other Australian container terminals in line with technology and ship size advances is expected to incur high costs (Arup 2017; Culley 2017). Replacing or upgrading large container handling cranes and automated container carrying equipment influences high retrofitting costs, which are unavoidable because ports must adapt to shipping industry requirements to remain competitive (Konings 2008; Justice *et al.* 2016).

2.2.3. Port transport and logistics vulnerabilities

Contemporary ports are vulnerable to disruptions within multiple logistics and transportation processes, and levels of vulnerability might vary extensively from port to port, and between critical actors within a single port (Crist 2003; Berle, Asbjørnslett & Rice 2011; Liu *et al*. 2018). These port transportation and logistics vulnerabilities exist within designated port lands and waters, and across the networks of crucial goods and services providers (Crist 2003; Hsieh, Tai & Lee 2014; Burns 2015). Port vulnerabilities increase under the influences of operational and geo-spatial changes that recast the freight task environment, the rapid pace of technology advances, urban encroachment on port boundaries, expansion of containerisation, supply chain operator requirements for increasing efficiencies, plus inter and intra port competition (Ducruet & Notteboom 2012). Competitive pressures increase port susceptibilities to business downturns, through regional road, rail and air freight agencies both supporting and competing with ports for intermodal cargo movement (Ng, Padilha & Pallis 2013). Conceptually, port failure after disruption might see business lost to either alternative freight agencies or to a competing port, to the port's longer-term business detriment. Alternatively, a major failure of regional freight agencies that support port business might leave the port unable to operate. In summation, port vulnerabilities are influenced strongly by the risk management performance capabilities of the port-centric integrated road, rail, air and sea alliances (Notteboom & Winkelmans 2004; Berle 2012).

Port vulnerabilities are addressed by multiple maritime and supply chain researchers (Berle, Rice & Asbjørnslett 2011a; Chhetri *et al.* 2015; Brasington & Park 2016; Pitilakis *et al.* 2016; ZIO 2016; Lantsman 2017; Liu *et al.* 2018) but port

vulnerabilities are rarely mentioned in community disaster response literature. This is a surprising omission when arguably, emergency aid logistics might best be transported by sea when regional transport systems are disrupted – this occurred following Cyclone Tracy, which devastated the Australian city and port of Darwin in 1975 (Scanlon 1996; Pettit & Beresford 2005). This omission may be due to a potential disconnect between the maritime emergency management and community disaster streams of research. This risk management disconnect is identified in Wakeman's (2013) analysis of New York-New Jersey Port and regional emergency management capabilities following Hurricane Sandy.

Conceptually, this section provides evidence that Australian ports exist within dynamic and complex operating environments, with vulnerability sensitivities to diverse risks both within these ports, and within their external networks of crucial goods and services providers. Port management preparedness to meet these systemic complexity challenges requires strong and informed risk management leadership (Hellingrath *et al*. 2015).

2.3. Port stakeholder vulnerabilities

From supply chain and national economy perspectives, the port is a sensitive logistic node due to the concentration of vital intermodal activities in the one location, effectively transforming the port into a maritime trade bottleneck (Trepte & Rice 2014; Kuo, Lin & Lu 2017). Port critical operations and services are enabled by logistics functions, intermodal transport, port land and sea operational resources, and the continued availability of critical assets and infrastructure (Burns 2015). As the volume of seaborne trade continues to grow, global supply chains become increasingly vulnerable to disruptive shocks at sensitive logistic nodes (Breur *et al.* 2013).

The end-to-end supply chain is comprised of multiple logistics networks whose nodal junctures (some critical) represent points through which cargo or passengers must pass, or where a crucial process or transportation change must occur (Blecker, Kersten & Gertz 2008). Examples of logistic nodes include factories, warehouses, container terminals, intermodal freight centres, passenger terminals,

and the port itself (Rodrigue, Comtois & Slack 2009). The port can be described as a complex regionalised system, which collectively comprises a critical services node that is integrated with and adds value to multiple supply chain port users (Robinson 2002; Panayides 2017). Port system reliability depends upon interconnectivity and interdependencies between critical infrastructure nodal clusters (Chen 2016). Critical nodes within transportation and logistics networks represent vulnerability points (bottlenecks) at which a disruption might bring the entire network, including the port, to a halt (Rodrigue & Notteboom 2017).

Potential points of failure can be illustrated in the form of a diagram that illustrates the path of port business through critical nodes, where within this study, the port system extends across the hinterland, incorporating critical logistics, transport and infrastructural nodal clusters connected to the port by physical and virtual linkages (Heilig & Voß 2017b; Rodrigue & Notteboom 2017). These lines of connectivity link together the port's supply chain components, which are shown in Figure 2-2 as critical nodes (black) and edge nodes (grey).

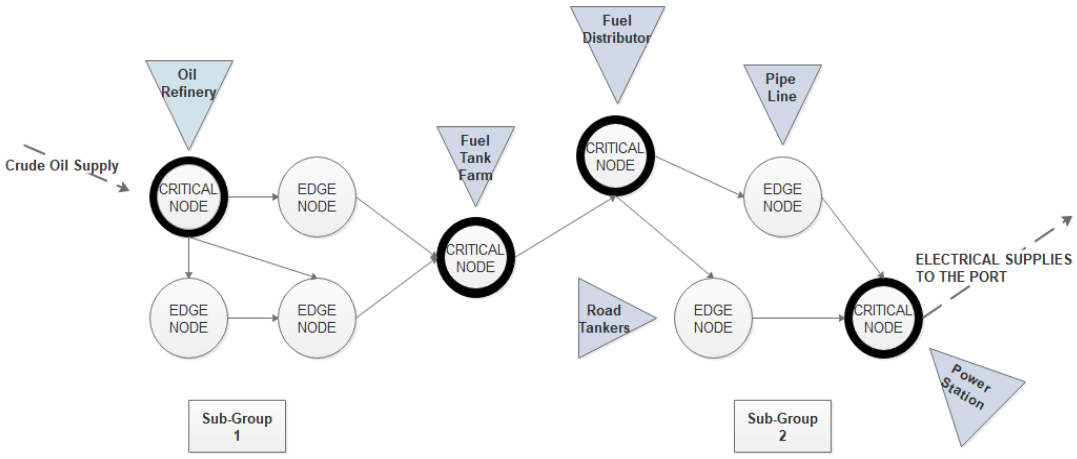


Figure 2-2: A logistics network segment – example of critical nodes as potential bottlenecks (Author).

This representation is a simplistic application of graph theory, which is receiving wider use in identifying complex network properties including clustering, connectivity and vulnerabilities (Phillips, Schwanghart & Heckman 2015; Chen 2016). Figure 2-2 represents the energy flow across the port network, whereby an oil refinery receives crude oil from the port and then processes the crude oil into fuel products. Fuel makes its way through storage and distribution linkages to the

power station which then supplies the port. Interdependencies and interconnectivities between nodal clusters create efficiencies but individual vulnerabilities might lead to cascading network failure (Ouyang 2016).

Chen (2016) discusses how each networked cluster relies on edge nodes for its provision of critical products, services and information, and the failure of edge nodes might result first in localised failure and then consequently, network failure. Effectively, external agency vulnerabilities and risk management shortfalls become port vulnerabilities.

2.3.1. Port-centric cluster vulnerabilities

Port risk management literature provides scant recognition of vulnerabilities and relationships at risk within the port-centric clusters of critical goods and services suppliers. Logistics, transportation and informational relationships might occur between port-centric cluster members in top-down/bottom-up, horizontal and circular patterns as indicated in Figure 2-3 which is based upon nodal relationship studies by Narkhede, Patil and Inamdar (2014), and Quéro and Dupont (2017).

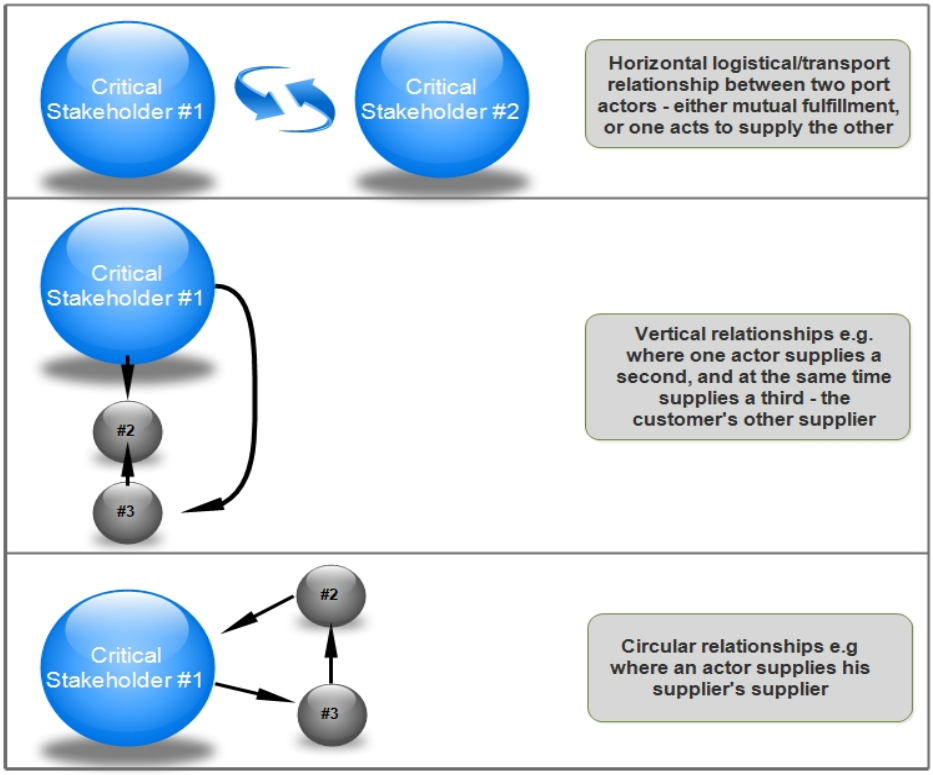


Figure 2-3: Supply flow connectivities representing potential vulnerability loci between the port's networked stakeholders (Adapted from Narkhede, Patil and Inamdar, (2014; and Quéro and Dupont, 2017).

Cluster analysis within socio-ecological systems is argued to be a useful method by which networked critical connectivities and vulnerability profiles are identified and assessed (Kok *et al.* 2015). Ports might have numerous cluster relationships. Donahue and Moore (2012) describe ports as complex organisations with network structures composed of many interconnected public and private sector actors. These actor interactions during a disruption event contribute to cluster vulnerability if rapid adverse changes cascade from actor to actor across the operational task environment. If a domino-like process of port-centric industry failure occurs across port-centric supply networks, then the resilient port must be able to sustain some level of damage and yet continue operating (Carvalho, Lamkin & Perez 2012). Port-centric cluster vulnerabilities arise when the port's holistic risk management strategies become (or are initially) fragmented because of various critical stakeholder self-interests that may or may not coincide (Bichou & Gray 2005). Opportunities for collaborative and connective port actor risk management behaviour might only occur within short term and flexible opportunistic alliances, during which the degree of information sharing may be limited (Peterson, Wysocki & Harsh 2001; Wysocki, Peterson & Harsh 2006).

Port-centric cluster networks and their vulnerabilities are rarely studied within an Australian context. Singh, Chhetri and Padhaye (2016) explore port-centric logistics and transportation clusters in case studies related to container ports Melbourne, Botany Bay and Brisbane. They observe that cluster membership is dominated by road freight transport participants and estimate that, from 2006 government statistics, a total of 719 port-centric firms provide critical goods and services to Melbourne, Brisbane and Botany Bay, with a combined income of A$93 billion. The scale of business undertaken by these firms indicates their large and important roles in supporting port operations, whereby underlying network risks to intra-cluster performance might also harm port performance (Chen 2016; John *et al*. 2016; Ongkowijoyo & Doloi 2018). Arguably, as a port's external stakeholder numbers increase, so too does port vulnerability. This is an outcome of larger organisational network size, greater number of interconnections and cross-sectoral interdependencies, and increased systemic complexity (Choy *et al.* 2007;

Lovrić, Blainey & Preston 2017). In the case of Australian ports that export crude oil and gas, port external risk vulnerabilities might also include offshore and subsea industry participants and the associated infrastructure connecting the port to offshore oil and gas fields (Hayes 2014; Renn 2014; Abdussamie *et al.* 2018).

A need exists to collaborate in and coordinate risk management efforts across organisations and sectors during a disaster (Abbas, Norris & Parry 2018; Friday *et al.* 2018). When an emergency event escalates and involves more organisations, a number of these additional entities will be unaccustomed to emergency management processes, thereby making emergency management coordination, collaboration and response increasingly difficult but more necessary (Owen *et al.* 2016; Abbas, Norris & Parry 2018). Network risk management collaboration impediments might include generally uncoordinated behaviour, constrained interactions and communication, and minimal risk treatment cooperation which add complexity, uncertainty and increased vulnerability to a port's risk management preparedness (Fenwick, Breville & Brunsdon 2009; Abbas, Norris & Parry 2018). Port stakeholders may be reluctant to enter enduring organisational risk management relationships with the port (Waters 2011) and when having ability to partially or fully control a risk, may not accept responsibility or feel compelled to manage or communicate these risks to the benefit of an external organisation (Handley-Schachler & Navare 2010; Hopkin 2017).

Additionally, actors may be disinclined to accept legal or financial liabilities for implementing risk management solutions that may benefit others. Nonetheless, cluster network actors and other ports might assist port emergency responses through contributing additional external management resources and personnel support (Hiles 2011; Rose, Wei & Paul 2017). Australian nation-wide port cooperation and assistance is notably present during the management of oil spill emergency events and exercises, primarily the result of a formal framework established by government across diverse public and private sector organisations (AMSA 2017; Miller & Quinn 2017).

2.3.2. Port stakeholder uncertainties

Ports operate under high levels of uncertainty related to complexities and ambiguities arising within the interrelationships and interdependencies between multiple independently motivated stakeholders (John *et al.* 2015). A US study (Southworth *et al.* 2014) finds that ports experience unique challenges to their risk management effectiveness due to complex physical, transactional, and institutional interconnections and interdependencies with their networked stakeholders. Southworth *et al.* (2014) argue that overcoming these impediments requires coordination of stakeholder risk management efforts across multiple logistics and transportation operations and their enabling service providers.

On one hand, stakeholder interdependencies are perceived to potentially exacerbate disruption consequences through the network ripple effect of hazard impacts (Ivanov, Sokolov & Dolgui 2014; Dolgui, Ivanov & Sokolov 2017). On the other hand, stakeholder interdependencies in the form of coordinated, cooperative and collaborative risk management responses contribute to making a port system more robust and resilient (Hambridge, Howitt & Giles 2017; Wan *et al.* 2017; Whelan 2017). This perceived value in coordinating stakeholder risk management efforts (Southworth *et al.* 2014) is reiterated by Friday *et al.* (2018) who describe relational risk management arrangements as a synergistic interfirm process of collaborative risk management (CRM). Friday *et al.* (p. 238) conduct a literature review encompassing 101 peer-reviewed articles that were published over 21 years, and propose a strategic relationship definition from current relational view theory that might also align with port stakeholder risk management relationships:

> Collaborative risk management is an interactive process based on mutual commitment between firms with a common objective to join effort and mitigate supply chain risks and related disruptions through co-development of strategic relational capabilities and sharing of resources.

Lacking collaborative risk management processes and procedures, individual stakeholders might then follow different and possibly conflicting business

continuity and disaster recovery aims, methodologies and estimates of recovery times (Hamilton 2011; Hiles 2011; Losada, Scapada & O'Hanley 2012; Wakeman 2013). Accordingly, collaborative risk management across a large network of port-centric stakeholders is a potentially daunting challenge, one alternatively described by Hamilton (2011) as multilateral continuity planning. Hamilton warns that individual self-interests usually run counter to collaborative business continuity planning, and because port managers are unaware of how underlying stakeholder self-interests might manifest, then potential exists for risk management uncertainties to expand.

From a system behavioural context, human response under stress, complexity and ambiguity is described as unpredictable and uncertain (Kyoto University 2009). In this regard, Van der Vorst and Beulens (2002) argue that port organisational uncertainty has four primary origins. This uncertainty arises from *diverse port actor objectives* associated with commercial self-interests, *indistinct knowledge* concerning the port's operational environment, the *unpredictability of likely actor behaviour* in the event of severe stress or disruption, and *unclear lines of port network controllability and leadership*. Additionally, if a disruptive event forces the closure of a port, then the extent of the disruption damage, the failure duration, and the likely disruption effects on port stakeholders add to an already uncertain situation.

Uncertainty-driven pressures potentially affecting port stakeholders are related to an increasing rate of globalisation, the rapid pace of technical innovations, difficulty in ensuring unimpeded informational flow, the post 9/11 need for enhanced security measures, and the increasing complexity of networked agencies (Mason-Jones & Towill 1998; Cova & Conger 2004). Maritime transportation uncertainty might manifest itself in the supply chain value stream in the form of port disruptions, thereby increasing costs, creating delays, and adversely impacting supply chain effectiveness and efficiency (Mason-Jones & Towill 1998; Choy *et al*. 2007; Sanchez-Rodrigues 2009). Operational uncertainty arising within the port community of actors involves subjective factors and random variables that may be difficult to measure and analyse under any

situational model (Ayyub & Klir 2006). This uncertainty might increase in situations when an event affecting one actor might impart major effects on others within the same tightly coupled network.

The existence of unknowns, unexpected events and uncertainties provide dimensions of risk that are intrinsic to tightly coupled complex systems (Weick & Sutcliffe 2015; Haimes 2008). Tight coupling arises from organisational interconnectedness, and the term implies relational criticality between networked stakeholders (Hartwich 2012). An example of tight coupling and relational criticality is the relationship between fuel providers and towage service operators, where without fuel the port is without tugs and may not be able to operate until fuel supplies return (Lowinger, Cwilich & Buldyrev 2016). Tightly-coupled and interactively-complex organisational relationships are argued by Perrow (2011) to be at greater risk to disruptive events than less integrated organisations. An extension of this argument might be that Australian port managers should consider making their organisations less integrated with their stakeholders, however, the concept of minimising interactively-complex organisational relationships within the port supply chain to reduce risk is not a practicable solution. Instead, port managers must endeavour to better understand their internal and external areas of vulnerability and develop risk management profiles to match. This establishes a need for the next stage of research exploration, in investigating the port risk environment for hazards that might exploit port vulnerabilities.

2.4. Summary

Chapter 2 provided an examination of Australian port operations and multiple factors that contribute to failure modes and vulnerabilities. Failure modes and vulnerabilities subject to disruption carry potential to impact upon port business continuity, leading to constraints or a halt in port business. Australian ports are highly valuable national critical infrastructure, comprising regionalised complex systems of interrelated and interdependent logistics, resource and transportation actors. The literature reveals that the extended nature of the port's own supply

chain and its external stakeholders renders it increasingly vulnerable to uncertainties and disruptions. These disruptions might either impact the port directly, or by ripple effect through the consequences of failure involving second or third parties of crucial importance to port operations. The following chapter extends this exploration of port vulnerabilities, risk identification and assessment, by examining the characteristics of hazards that might be encountered within the port risk environment.

Chapter 3: The port risk environment

3.1. Introduction

The previous chapter identified Australian port characteristics and their importance as national and regional critical infrastructure. Discussion included how ports have become more operationally complex with increasing reliance upon technology, specialised equipment and infrastructure, and dependencies upon their networks of critical goods and services suppliers. Having identified major port vulnerability factors in Chapter 2, this chapter now demonstrates how ports have become progressively at greater risk to emerging and increasingly severe low probability/high consequences disruptions. Port managers may never resolve this challenge, which might instead only be managed and mitigated. This is because port risks are of a dynamic nature, often with multi-hazard/multi-risk implications (Kappes *et al.* 2012; Fleming, Zschau & Gasparini 2014; Lam & Lassa 2017). The port risk management task is made increasingly complex by the proliferating and evolving nature of global risks (WEF 2018). The changing nature of port risks is demonstrated by port exposure to increasingly severe adverse natural events and changing climate patterns (Lam & Lassa 2017). Port hazards are explored firstly from a global perspective, and then with reference to how similar hazards might challenge Australian port operations. The literature is examined for risk management techniques that port managers might employ in identifying and preparing for these hazards. Chapter 3 begins with an overview of the port risk environment, followed by a clarification of port risk management terminology.

3.2. Port hazards and risk

The Australian Institute for Disaster Resilience glossary (AIDR 2018, n.p.) describes a hazard as:

> A potentially damaging physical event, natural phenomenon or human activity that may cause loss of life, injury or other health impacts, property damage, loss of livelihoods and services, social and economic disruption or environmental damage.

The relationship between hazard and risk is descried (AIDR 2018, n.p.) as follows:

> "Risk" refers to the likelihood that a hazard will happen, its magnitude and its consequences. It relates to the probability of external and internal threats (such as natural hazards…) occurring in combination with the existence of individual vulnerabilities.

Ports are identified as high-risk places within the transportation chain (Berle, Rice & Asbjørnslett 2011a, 2011b; Southworth *et al.* 2014; Stažnik, Babić & Bajor 2017). Hazards and emerging risks that challenge port managers increasingly change and are becoming harder to predict, however the adverse consequences are likely to share some commonalities with port risks in general (Beasley & Frigo 2010). Ports are exposed to numerous hazards at any one time, hence port risk managers might adopt a multi-hazard and multi-risk mindset, rather than treating each hazard and corresponding risk as a single risk management factor (Kappes *et al.* 2012; Fleming, Zschau & Gasparini 2014). Multiple risks might combine, for example strong winds/heavy rain plus flooding/sea rise from a tidal surge. Alternatively, a triggering event of one causality might initiate multiple other risk events and outcomes. Consequences of a multi-hazard event are demonstrated by the 2011 Japanese east coast earthquake, which translated into tsunami waves, devastation along the affected coastline and hinterland, consequential seawater pollution, loss of all local utilities and services, damage to a nuclear power station cooling system and core meltdown, and eventual regional land, air and sea radiation contamination (Wang, Kato & Shibasaki 2013).

Coupled with multiple sources of risk to which complex port operations are customarily exposed, new and emerging hazards plus increasingly severe natural events (WEF 2018) test the effectiveness of risk management strategies and processes. As described by the Australian Government (AG 2017, p. 7) '…disruption to our most critical ports could have wide-reaching impacts on the economy'. Localised port disruption consequences could result in injuries, illnesses, fatalities, infrastructure and asset harm, environmental pollution, direct and indirect economic losses, unemployment and plant shutdowns (Rose 2009; Rose & Wei 2013; Southworth *et al.* 2014). Externally, port failure is likely to impact on other industries through interconnectedness between critical

infrastructure, whereby failure passes by a ripple effect from network to network (Hartwich 2012). Efforts to better understand the risk environment and to minimise port failure and reduce downtime can benefit the national economy. For example, Australia's major resource export ports are primarily located in the north Australian cyclone belt, and cyclone-related loss of trade from major resources export ports could cost the national economy as much as AU$3 billion in one year (Ng. *et al*. 2013a; Cahoon *et al.* 2015, 2016). As a first step in understanding this port risk environment, it becomes constructive to understand risk terminology.

3.3. Exploring the terminology

Few studies have been conducted on the extent of Australian port management knowledge of and familiarity with risk management terms, or the level of risk management qualifications held by senior port executives. Delogu (2016) suggests that confusion between the terms hazard, danger, threat and risk arises because these terms are synonyms, as described in the Oxford Dictionary of English (Simpson 2018).

3.3.1. The concept of hazard

In narrower terms than the previously quoted AIDR (2018) definition of hazard at Section 3.2., Manuele (2013, p. 237) describes a hazard as '… any activity or technology that produces risk' and in the context of adverse risk, a hazard exists as 'the potential source of harm'. Green (2008b) defines hazard impact as an interrelationship between hazard power, its effects, and organisational vulnerability to the hazard. Green (2008b) notes that differences between an adverse event's impact and its consequences are blurred, however, an *impact* is relatively short-lived and localised. By comparison the *consequences* of a disruption might be experienced for a prolonged period within a single system or as it cascades across other interrelated systems (Hartwich 2012). The impact of an adverse event might be difficult to treat, however the severity of consequences from a port disruption might depend upon how effectively port managers cope with the disruption impact (Green 2008b).

Whereas a hazard and a threat both challenge port managers in the form of adverse risk, with commonalities in origin and outcomes, they differ in important aspects. The hazard represents the risk in a dormant state, whereas the threat represents an actualisation of the risk (Green 2008a). For example, a flammable ship's cargo represents a fire hazard, whereas the burning substance threatens the port's adjoining infrastructure and operations. Green (2008b) further describes a threat as being the operationalisation of vulnerability to a hazard, coupled with expectations of how the hazard might impact the organisation. As port managers must rely on their subjective expectations for gauging hazard consequences, risk management becomes associated with uncertainty.

3.3.2. The concept of traditional risk management, and beyond

Port managers practising traditional risk management approaches engage in risk identification and assessment workshops, from which expectations of risks might be identified through qualitative brainstorming processes or quantitative analyses of a known risk environment (Srikanth & Venkataraman 2013; Haimes 2016). According to Aven (2016), scientific research into risk assessment and risk management that began some 40 years ago provides the foundation for present risk management processes and procedures. By comparison with today's evolved scientific perspective of what constitutes risk, the early foundational scientific perspectives of risk constitute a quite narrow world view of risk assessment and of how risk might be managed (Tang & Musa 2011; Flage & Aven 2015; Aven 2016). Early researchers ascribe risk with the traits of simplicity, singularity, surety and clarity, for example their probabilistic definitions include: 'risk is a measure of the probability and severity of harm… (and) a thing is safe if its risks are judged to be acceptable' (Lowrance 1976, p. 8) and '…risk is the probability of an adverse outcome' (Graham & Weiner 1995, p. 30).

Traditional risk management as a probabilistic concept is more closely identified with the known properties and outcomes of risk than with uncertainties (Perera & Higgins 2013). As previously discussed in Section 2.3 from a port vulnerability context, uncertainties relate to known outcomes (consequences) but unknown probabilities, and in recent times risk uncertainties have become associated with

emerging risks (Flage & Aven 2015). Emerging risks (IRGC 2011, p. 4) are considered to arise within three categories:

a. Risks with uncertain impacts, with uncertainty resulting from advancing science and technological innovation;
b. Risks with systemic impacts, stemming from technological systems with multiple interactions and systemic dependencies; and
c. Risks with unexpected impacts, where new risks emerge from the use of established technologies in evolving environments or contexts.

The consideration of risk uncertainties, unknowns and unexpectedness lead this thesis towards a categorisation of risk characteristics that are attributed to Rumsfeld (2002, p. 47):

> There are known knowns; there are things we know we know. We also know there are known unknowns; that is to say we know there are some things we do not know. But there are also unknown unknowns – the ones we don't know we don't know.

With scientific and management acceptance of risk uncertainty characteristics (ISO 31000:2018) the port risk management literature has come to reflect the first two characteristics (known knowns, known unknowns). Within this thesis port failure modes discussed include stakeholder vulnerabilities (Section 2.3.) which, while presumably known to the stakeholders, may not be known to port managers. Hence, for port managers a further category of unknown knowns is argued to exist, and the scope of unknown knowns might be broadened by managers discarding cognitively unlikely scenarios within risk identification workshops as described by Srikanth and Venkataraman (2013) and Haimes (2016). The scientific recognition of emerging risks and associated levels of uncertainties introduces to port managers a further risk category of ‘unknown unknowns’ whose unidentified or unidentifiable risk characteristics might include unforeseeability, unexpectedness, uncertainty, unfamiliarity, or sudden change

and/or increased severity in the properties of an existing risk (Bralver & Borge 2010; Kim 2012; Flage & Aven 2015).

3.3.3. Deep uncertainty

The standard for risk management, ISO 31000:2018, departs from the customary practice of defining risk as a function of a hazard's predicted probability multiplied by expected consequences (Altiok 2011), and instead associates a hazard with the effect of uncertainty upon an organisation's objectives. Port operational risks are associated with 'known unknowns' whereby a port manager knows, for example, that the cyclone season is due to begin (a 'known'), but unknowns include whether a major cyclone will eventuate during the season, whether one will impact the port, or what scale of damage might result. Deeper uncertainty arises with new and emerging unforeseen risks, whose indeterminate characteristics involve 'unknown unknowns' and this deeper uncertainty (Aven & Krohn 2014; Aven 2017) exposes port managers to cognitive biases and deficiencies in their probability judgements (Wucker 2018). Cognitive biases and deficiencies related to probability judgement concepts and port risk-related uncertainties might arise if managers are unaware of, or have overlooked, previously unknown and unexpected emerging risks (Faulkner, Feduzi & Runde 2017).

If deep uncertainty arises because the characteristics of new and unexpected hazards might only be conjectural (Faulkner, Feduzi & Runde 2017; WEF 2018), then port managers are exposed to non-reducible physical variabilities of the risk environment (aleatory uncertainty). Alternatively, deep uncertainty that results from management overlooking, or only acquiring partial risk knowledge (epistemic uncertainty) can be addressed to reduce this level of risk exposure (Borgonovo 2017; Borgonovo *et al.* 2018). Epistemic uncertainty, which relates to missing information (Walker, Marchau & Swanson 2010) constrains a port manager's ability to fully understand the scope and severity of risk, even if the manager suspects that crucial information is missing from risk deliberations. If left unchecked, epistemic uncertainty hampers port risk identification, prediction, and risk treatment. Reasons for ignoring missing information might include port senior management being unwilling to explore possibilities for some low probability risks,

nor expending time and money on risk incertitude – an outcome that is sometimes termed subjective uncertainty (Paté-Cornell 1996; Ayyub 2014; Han, Mittal & Zhang 2017).

Epistemic uncertainty and ambiguity might also arise due to port managers not being fully cognisant of their internal and external organisational risk environments, possibly through management inability to understand or deconstruct layers of complexity within the cause-effect phenomenon, or through managers making incorrect assumptions or predictions of what constitutes risk (Renn 2011). From an epistemic discussion of port risk terminology, the research now examines the port organisational risk environment and its primary attributes.

3.3.4. Organisational risk environment

The organisational risk environment is comprised of *preventable risks* (failure in processes or human error), *strategic risks* (the competitive trade-off between risk and reward), and *external risks* beyond the organisation's capability to influence or control (Kaplan & Mikes 2012). Preventable and strategic risks are potentially controllable by conventional risk management techniques, whereas uncontrolled and unexpected external risks require adaptive organisational responses and innovative operating capability (Kaplan & Mikes 2012). For port managers this means that while conventional risk management processes are applicable to known preventable and strategic risks, the introduction of unknowns and uncertainties to the risk management problem demands either adaptation of existing risk treatments, or capabilities at a higher level than conventional responses should unforeseen and unexpected disruptions occur.

The organisational risk environment is dynamic, with new and emerging risks presenting differing risk management challenges to those of the past, and existing risks altering in terms of their frequencies and severity (Hopkin 2017; WEF 2018 Within port strategic planning tasks, a requirement arises to periodically review risk treatments so that they remain sufficiently flexible, adaptive and up to date to contend with inevitable changes within the port's internal and external operating environments (Hopkin 2017; Bichou 2018). Port managers might

struggle to maintain operational proficiencies as rapid technology changes occur within core processes, thereby increasing the port's exposure to hazards affecting that technology application (Neureuther & Kenyon 2009; Loh & Thai 2012; Bichou, Bell & Evans 2014). Increasing numbers and changing demographics of port stakeholders (Geerlings, Kuipers & Zuidwijk 2018) mean that interactions and interdependencies between the port and its hinterland cluster stakeholders create new mutual uncertainties and vulnerabilities (Tan, Lam & Zhang 2015; Singh, Chhetri & Padhaye 2016; Hopkin 2017). Additionally, like other organisations linked with global supply chains, ports are increasingly challenged by socio-political interventions and changing legislative compliance requirements (Hopkin 2017; Bak 2018). These indications of changing port risk patterns raise important questions regarding whether port managers understand these alterations in the nature, frequency and potential severity of risks, and if so, what strategic and tactical management changes Australian port managers might make in response. Associated questions include the potential roles of resilience in addressing port risk and vulnerability changes, and to what extent port managers might resist changes to their existing risk management processes and capabilities to avoid an inconsistent risk governance culture, to contain costs, or for other reasons. Additionally, with these perceptions of changing patterns of port risk, the discussion broadens to explore what changes new and emerging hazards might bring to port disruption consequences.

3.3.5. Relationships between port hazards and disruption consequences

Reason (2008) analyses a series of primarily ship-oriented port disruptions, and observes that three main factors contribute to accidents in ports:

a) ports possess inherently dangerous hazards such as rocks, shoals, tidal currents and fixed and moving objects that contribute towards ship accidents;
b) unsafe acts or less than adequate personnel performance create circumstances where accidents become more likely; and,
c) a port's exposure to hazards becomes magnified if risk management deficiencies exist, as manifested by dysfunctional safety culture, lack of

training or motivational forces, and unchecked erroneous human behaviour.

Contemporary port hazards differ from those in the past, for example the port's increasing reliance upon technology, socio-political hazards inclusive of activist groups, and increasingly severe natural events. However, the holistic nature of port hazards and disruption outcomes remains unchanged from those of a general nature described by Lowrance (1976). According to Lowrance these fall within the scope of:

a) new hazards of increasing scale and duration;
b) problems about which managers know little;
c) poorly understood aspects of weather-related hazards;
d) unknown side effects and unintended consequences of everyday activities and processes;
e) hazards with irreversible consequences; and,
f) widespread uses of technology without fully understanding resultant hazard vulnerabilities and consequences.

Global port hazards and disruption characteristics are drawn from the literature as shown in Table 3-1. The port hazard and vulnerability literature discovered by this study is more prolific within the categories of adverse natural events (geological and hydro-meteorological), technical and technological failures, and environmental issues. Keim (2015) investigates the occurrence of natural disasters during 1964-2013 and finds that these comprised 83% of all global disasters during the period, and that the number of natural disasters is increasing. Hydro-meteorological disasters headed this hazard category, with floods and drought causing most damage and losses (Keim 2015). The consequences of hazards such as these might be exacerbated by new vulnerabilities arising because of the evolution of port operational practices and the introduction of technological management techniques.

Port Hazard categories	Disruption characteristics	References
Operational	Port equipment failures, infrastructure failures, cargo spillage, ship accident	Burns, 2015 John *et al*. 2015
Organisational	Port congestion, labour unrest	John et al. 2015
Geological	Earthquakes, earth slippage, landslides, tsunamis, volcanic ash plumes	Blaikie *et al*. 2014 Joyce *et al.* 2014 Koschatzky and de Oliveira, 2016
Hydro-Meteorological	Avalanches, bush fires, climate variations, cyclones, dust storms, droughts, floods, hail, lightning, sand storms, storm surge, strong seas, super storms, thermal extremes, thunder-storms, stronger natural hazards, urban drought	Blaikie *et al*. 2014 Gaile and Willmott, 2005 Ammann, Dannenmann and Vulliet, 2006 Smith and Katz, 2013 Keim, 2015 WMO, 2017 WEF, 2018
Biological	Epidemics, pest attacks, viruses, invasive species, bio-weapons, marine toxins	Ammann, Dannenmann and Vulliet, 2006 Pernick, 2014
Technical and Technological	Chemical, industrial, nuclear, oil spill, radiological, power outages, hazardous materials, fire-prone construction materials, telecommunications failure, satellite communications failure, GPS failure, RFID failure, emergency communications failure, cyber security	Gallaire, 1998 Rubin, 1998 Mayhorn and McLaughlin, 2014 Smith and Katz, 2013 John *et al*. 2015 WEF, 2018
Security	Arson, chemicals and biological accidents, criminality, road and rail accidents, sabotage, terrorism, social disruption	Rubin, 1998 Mayhorn and McLaughlin, 2014 John *et al*. 2015 WEF, 2018
Financial	Cost overspend, fraud, theft, record keeping and storage safety, financial instability, banking transaction failure, financial information constraints,	Shiller, 2009 John *et al*. 2015
Socio-political interventions and influences	Change in political decisions, community opposition, strikes, protests, radicalism, seabed boundary disputes, ocean resource disputes, radicalisation of disaffected persons.	Paton, Kelly and Doherty, 2006 Guild, 2009 Dauvergne and LeBaron, 2014 Graham and Kaye, 2015 Anton, 2017 Boin *et al.* 2017
Environmental	Cargo contaminants, dust, underground seepage, regulatory compliance, reputational, climate change	Grech *et al*. 2013 Smith and Katz, 2013 Nyborg *et al*. 2016 Becker *et al.* 2018 Sierra *et al*. 2017 Kellman, Mercer & Gaillard, 2017
Security	Infrastructure and facilities incursions, information and data theft	Atlas, 2013

Table 3-1: Port hazards.

An issue in evaluating new vulnerabilities is that port risk management literature provides little guidance on compounding factors that might exacerbate the consequences of hazards, or of port managers' awareness and inclusion of this issue in their vulnerability identification and assessment processes. For example, the 2004 Aceh earthquake resulted in a tsunami that caused sea level oscillations of up to plus or minus one metre during a 72 hours period at Western Australian major resources export ports (Short 2006). Western Australian resources export ports employ Dynamic Under Keel Clearance (DUKC) software to calculate individual ship sailing draughts (Curtis 2017). The net clearance between a deep draught vessel's keel and the seabed is normally based upon PIANC guidelines (Gourley 2007), and net under keel clearance is suggested by PIANC (2014, p. 33) to be 'at least 0.5 m, but could be increased to 1.0 m where the consequences of touching the bottom is large (e.g. for channels with rocky bottoms)'. However, unexpected sea level oscillations, for example from a tsunami, might negate this planned net clearance between a ship's keels and the seabed.

Port risk management literature also provides scant guidance on whether path dependencies might influence port risk attitudes and management willingness to explore new areas of vulnerability. If path dependent processes and procedures are effective under circumstances of organisational stability, then the question arises of whether the organisation might lack sufficient agility and flexibility in meeting disruptive change and particularly, sudden disruptive change.

3.3.6. Sudden disruptive changes and path dependency

Winn *et al*. (2011) describe sudden disruptive changes as low probability/high consequence events that '…may range from short, extreme events to sustained long-term impacts' with immediate direct or indirect consequences, and with '…potential to exceed thresholds and tipping points'. Examples of sudden disruptive change include earthquakes, tsunamis, severe weather events, financial shocks, wars, and catastrophic cyber-attack (Rosenoer & Scherlis 2007; Winn *et al.* 2011). The importance of sudden disruptive changes in comparison with other longer-term risk onsets, is that port risk managers may experience difficulties in responding to sudden disruptive events if they are resistant to change or

adherents of management path dependency (Everett 2003a; Zschau & Fleming 2014).

Path dependency is described as 'the tendency of persistence and self-reinforcement of paths and, by implication, the difficulty of changing a path once chosen (Wiering Liefferink & Crabbé 2017, p. 3). Barnett *et al*. (2015) argue from a climate change context that changes away from path dependency are required to make Australian public and private sectors more adaptable in managing risk. They maintain that path-dependent institutions adapt more slowly to change than the speed at which actual conditions are altering. Zhang, Ng and Becker (2017) also argue from a climate change context that port path dependencies constrain the building of resilience levels.

A path-dependent organisation could discover that reliance upon existing risk management practices is insufficient to cope with a sudden onset disruption. In such circumstances the organisation might no longer manage as before and must find new ways for coping with changing operational circumstances. Effectively, the organisation has been transposed past its critical threshold of change (Wilson 2012; Barnet *et al*. 2015). A sudden disruption and changing circumstances might occur if risk managers overlook or ignore early warning signs of a disruption, whereupon a time lag is created between disruption impact and management's disruption response (Booth 2015). Management becomes committed to an initial normal course of action, but if the nature of the disruption subsequently alters or initiates other consequences (IRGC 2011), then a second ineffectual time lapse eventuates until management regroups and alters their response - two disruptive-led sudden changes to port operations within a short space of time.

Sudden change also requires managers to work faster, thereby losing sight of strategic issues, overlooking vital information, and narrowly focussing on intuitive rather than rational responses (Booth 2015). Cyber-threats provide an example of path-dependent port managers being unable to manage hazard consequences, and then requiring reactive measures to regain organisational stability.

Beaumont (2017) argues that port operators, despite their high level of ICT dependency, are prone to overlook or ignore the need for cyber-security vulnerability assessments and disruption preparedness. Beaumont (2017) describes this behaviour as a fundamental lack of awareness of the level of threat and preparedness measures. A denial of service attack upon port systems and technology dependent infrastructure and equipment could result in a halt in port operations for an indeterminate period, from days to weeks. A State actor might launch such an attack upon another nation's critical infrastructure in political retaliation, as with the reported Russian State-sponsored attacks on Australian public and private sector computer systems following US, UK and French attacks on Syrian military assets (Borys 2018).

The inherent problem of path-dependent port risk management is conceptualised by visualising the port as a stochastic system with potential alternative responses to a denial of service attack. A 'ball and cup' regime shift analogy (Nolting & Abbot 2016) represents what happens when port risk management capabilities become overwhelmed by the disruption as shown in Figure 3-1. If port managers were well prepared over time to meet such an attack, then proactive defences and effective risk management processes against denial of service attacks might permit retention of existing status or allow a controlled positive shift in organisational capabilities and adaptiveness to an alternative but still acceptable operational status. Otherwise, a sudden disruption might cause the port to quickly reach a tipping point where management loses control over events. Figuratively the port is then transposed across an operational threshold until (perhaps days or weeks later) it eventually achieves stability within new operating circumstances as shown in Figure 3-1. If port managers find these new circumstances undesirable, then much work is required to regain stable operational capabilities. In planning and strategising to cope against potential hazards, port managers must identify and assess all feasible risks, including cyber-security.

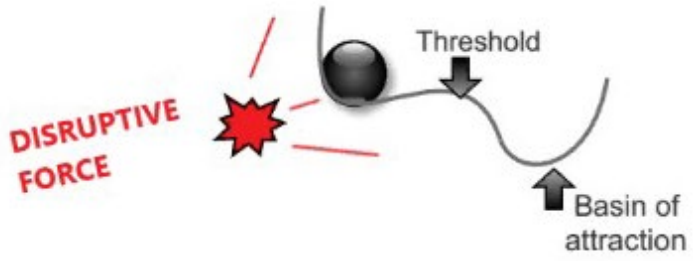


Figure 3-1: A hypothetical organisation subjected to denial of security attack, and potential transition to new operating circumstances (Adapted from Gunderson, 2000).

3.3.7. Port risk identification and evaluation

Risk analysis is a means of making sense of and coping with the organisational internal and external risk environment, and for reducing risk complexity, uncertainty and ambiguity (Modarres 2016). Through risk analysis, hazards and their characteristics are identified, quantified, ranked and assessed, following which the organisational risk managers establish appropriate risk treatments to control, mitigate or transfer these risks (Bichou, Bell & Evans 2014; Modarres 2016). In the case of Australian port authorities, risk analyses take place within annual brainstorming sessions (Srikanth & Venkataraman 2013). Organisational risks may run into the hundreds, and each selected risk must be assessed and given a unique identifier, allocated mitigation treatment, and provided with a responsible person (often a department head) to monitor and manage that risk (Mutton 2012). The risk register is usually constructed upon a software program that facilitates regular revision of risk updates, incident occurrences, mitigation efforts, and data input to the port authority auditing processes (Mutton 2012).

Management treatments of potential hazards are shaped by their levels of risk management learnings and a derived risk-centric knowledge base, organisational resources, objectives and risk tolerances (Scott *et al*. 2013; Aven 2016). Tolerance for some port risks might be lower than others, while some low probability risks might be neglected altogether (Sunstein 2002; Scott *et al*. 2013). For example, nil tolerance might be held for hazards that threaten life or personnel safety, whereas seismic hazards might be disregarded from within a normally earthquake free region. Managers might also disregard or overlook very low probability hazards as a non-credible threat, or perhaps under-invest in risk treatment, rather than

address problems that might manifest under specific circumstances (Sunstein 2002; Jonkeren & Rietveld 2016). Alternatively, risk managers might over-react to a low probability hazard due to what Sunstein and Zeckhauser (2011) describe as 'action bias' to risks with emotive consequences, for example gunman attacks.

Port risk managers must make judgements on whether and how to treat hazards and vulnerabilities based on evidence and value-based considerations (Aven 2016). If a port manager lacks the necessary knowledge and skills then he/she will be hampered in undertaking evidence-based analysis of hazards and vulnerabilities, and in assessing how this information correlates with wider information from other sources to potentially affect risk outcomes. The identification and evaluation of hazards might then be undertaken upon a value-based pathway and the important integration of facts, possibilities and values excluded from the decision-making process (Hansson & Aven 2014; Aven 2016). Value-based judgements on hazards and vulnerabilities rely on experience, however the port manager may not possess the requisite experience to exercise sound judgement, or, a specific category of risk has either not been experienced by the managers or may constitute a new, unforeseen and problematic risk (Gharehgozli *et al*. 2017). Subjective values-based risk management decisions might variously lead to organisational inaction, under reaction, or over reaction and hence the importance of adequate training and qualification to conduct evidence-based evaluation of risks and vulnerabilities. A suggested outline for port risk decision-making processes is shown at Figure 3-2.

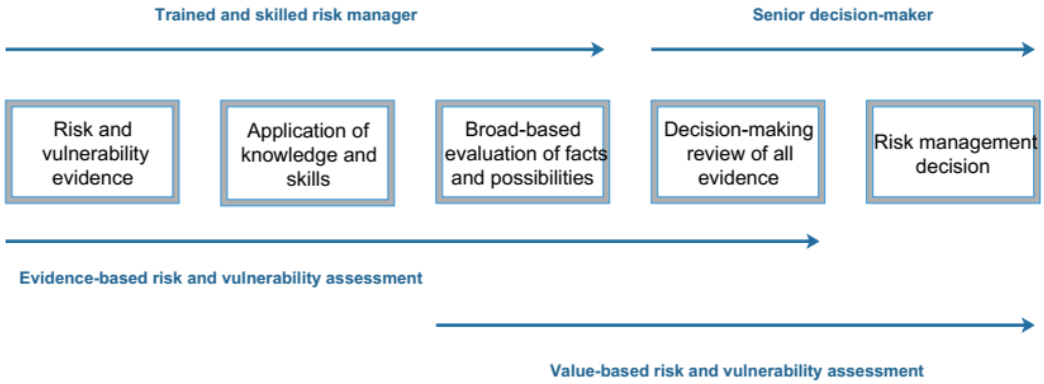


Figure 3-2: Evidence-based and value-based risk and vulnerability evaluations (Adapted from Aven, 2016).

In striking a balance between underacting and overreacting to low probability hazards, Manuele (2003) argues that a theoretically ideal situation exists when all known risks from hazards are reduced to an acceptable level. Even if known port risks are reduced to their lowest practicable level, a sense of uncertainty might ultimately prevail, because potential remains for unknown and unexpected organisational risks to exist (Weick & Sutcliffe 2015). Low probability/high consequence risks as an Australian port management concern are central to this study's research problem.

3.3.8. Port risk management leadership and governance

Port leadership, governance and organisational management capabilities are crucial capabilities in enabling effective organisational risk management and abilities to maintain business continuity during crises (Tarrant 2010; Mauelshagen 2012). However, assessing the qualities of holistic port leadership and organisation culture is a difficult process due to the complex interactions, interdependencies and collaboration between the many parties and networks that are necessary to fulfil key port roles, capabilities and functions. The port system is a multi-layered and complex organisation, comprising networks of logistics, macro and micro economic, supply chain, industry cluster, public and private sector, transportation, and infrastructure/asset interests (Burns 2015). This holistic port system appears to operate without directions from a central governance and leadership source, and Burns (2015) makes a clear argument that today's complex and turbulent port operating environment requires managers who can provide effective leadership and governance direction, and who can provide innovative, flexible and adaptable responses to operational, risk management and emergency response challenges.

Individual ports support many supply chains that engage with multiple goods and service providers, and when these providers interact with the port system, overlapping networks of roles and alliances are created (Sporleder 2006; Heaver 2009). The port's regionally extended and complex system might incorporate many industry clusters and perhaps hundreds of stakeholders (Chacon *et al.* 2012; Vonck & Notteboom 2016). This systemic complexity and multiple sources of vulnerability lends importance to port risk managers developing analytic risk

management, collaboration and communication skills of a high order (Pallis & Kladaki 2016), and in this context, education becomes increasingly important in augmenting risk management capabilities for port managers (Hopkin 2017).

Port leadership in stakeholder risk communications and collaboration is an important risk minimisation factor. Risk communications and collaboration across port stakeholder networks are impeded by public and private sector organisational level silo behaviour, and within other sectors the failure to share information has even led to loss of life (Allen, Karanasios & Norman 2014; Mikes & Migdal 2014; Karlsson *et al.* 2017). Inter-organisational lack of information sharing is also argued to impede the formation of systemic resilience (Fenwick, Seville & Brunsdon 2009; Li *et al*. 2017; Shaw, Grainger & Achuthan 2017). Silo behaviour is exemplified by limited connectivity between actors and agencies and results in uncoordinated behaviour, minimal communication, and only nominal cooperation. This characteristic is described as occurring within organisations, between organisations, and between disciplines (Fenwick, Seville & Brunsdon 2009). Silo behaviour raises the risk of organisational dysfunction, and behavioural influences include individual, organisational or geographical parochialism, and self-interest tensions between multiple businesses and professions (Schein 1996; Guelke 2005; Mikes & Migdal 2014). As with organisations in general, port actor silos and a divergence of stakeholder interests impact on the effective performance of risk management, business continuity and resilience (Christopher 2010; Straube, Nagel & Rief 2010; Waters 2011).

3.4. Understanding risk at Australian ports

Risk, according to ISO31000:2009, is defined in terms of the effect of uncertainty on objectives. Uncertainty is a central concept within the annual World Economic Forum report on global risks (WEF 2018, pp 6-7) which notes that organisations are increasingly and systemically challenged by:

> Proliferating indications of uncertainty, instability and fragility…(and)…that risks can crystallize with disorientating speed. In a world of complex and

interconnected systems, feedback loops, threshold effects and cascading disruptions can lead to sudden and dramatic breakdowns).

The WEF report is based on surveys and round table discussions on potential forthcoming risks, and concludes that societal, political, environmental, technological and economic hazards are the most likely forms of impending risk. A summary of the ten most likely risks to challenge global organisations, plus the top ten risks assessed for their likely impact (WEF 2018) are shown in Table 3-2.

Order of likelihood	Most likely disruption types	Disruptions with most impact
1	Extreme weather events	Weapons of mass destruction
2	Natural disasters	Extreme weather events
3	Cyber-attacks	Natural disasters
4	Data theft or fraud	Failure of climate change mitigation and adaptation
5	Failure of climate change mitigation and adaptation	Water crises
6	Large scale involuntary migration	Cyber-attacks
7	Man-made environmental disasters	Food crises
8	Terrorist attack	Biodiversity loss and ecosystem collapse
9	Illicit trade	Large scale involuntary migration
10	Asset bubbles in a major economy	Spread of infectious disease

Table 3-2: Predicted global risks (Adapted from WEF 2018).

Some disruptions from this list are considered to have potential relevance to critical infrastructure inclusive of ports and provide a basis for further port risk management research. The WEF (2018) guidance identifies contemporary hazards and risks that represent appropriate and relevant touchstones for investigating how vulnerable the ports consider themselves to be from each threat, their expectations of the hazards occurring in the future, and how effectively the impacts and consequences of these disruptions might have been managed in the past.

3.4.1. Port risk environment

The effectiveness of port management understandings of the risk environment, and potential consequences of disruption categories to port operations likely depends upon whether their evaluation is based upon an evidence or values-

based approach (Aven 2016). Renn (2014) argues that few risk decision-makers clearly understand their risk environment, within the context of:

a) *technological risks* that are new and emergent hazards arising from frontier practical science advances and processes;
b) *crystallising risks* that arise from introduced technologies and processes, but whose risks are recently recognised; and,
c) *aggravated risks* familiar to risk managers but whose likelihoods and/or impacts worsen over time.

An International Risk Governance Council (IRGC 2011) study suggests that organisational uncertainties and lack of clarity about the risk environment relate to the evolution of risks, which indicates that port managers who rely on experience when making risk management judgements may be technically disadvantaged. It is unclear to what extent Australian port managers understand the nature of evolving risk characteristics, when IRGC (2011) and WEF (2018) studies suggest that the global risk environment is altering because of:

a) scientific advances and technological innovation, and because these risks are new, managers are uncertain of what adverse outcomes might arise;
b) systemic consequences and uncertainties, compounded because of multiple interrelationships and interdependencies across the system; and
c) unexpected and unwanted outcomes from use of technologies, which arise due to a changing operational environment or external influence.

Informed discussion on port risk management capabilities and abilities requires fresh insights into how port managers prepare for threats emerging from a dynamic risk environment, with specific focus on 21st Century risks that Boin (2004, p. 167) describes as 'unwanted, unexpected, unprecedented, and almost unmanageable'. If port managers lack a clear understanding of their risk environment, then their subjective probabilities assigned to risk assessments are flawed if these indicate a stronger level of knowledge than what is possessed (Aven 2016). Gaining an understanding of Australian port managers' risk interpretation skills lends context to this thesis discussion.

Emergence of new risks and the metamorphosis (aggravation) of existing risks into greater risks with unexpected consequences require innovative, more powerful risk identification capabilities (Renn 2014, 2017). Accordingly, organisational decision-makers must become competent in managing adverse changes from multiple sources, a competency necessarily acquired through experience, learning and research (Wachinger *et al*. 2012). Without such competency, port managers might react and respond to a situation at hand without sufficient consideration towards a problem's initial causal factors or point/s of origin (Geary, Childerhouse & Towill 2002).

3.5. Hazards experienced at Australian ports

Australian port hazards appear to differ little from their global counterparts, except in relation to their geographical setting. Northern Australian ports are vulnerable to cyclones, flooding, high temperatures and tropical disease (Kelly-Hope, Purdie & Kay 2004; Maunsell 2008; Russell *et al*. 2009; Ng *et al*. 2013a). East coast ports experience intense low-pressure storms and consequential flash flooding, high waves, storm surge and gale force winds (Mills *et al*. 2010; Johnson *et al.* 2015. Southern ports experience drought and both high and low temperature extremes (McEvoy *et al.* 2013). Capital city ports and ports in large regional centres experience urban encroachment pressures and compete with the community for road and rail use (Stanley & Hensher 2009; Kilgariff 2017). Urban encroachment (Kilgariff 2017) led to the Port of Sydney losing its general cargo infrastructure and operations to waterfront housing and non-maritime business premises.

According to Gharehgozli *et al*. (2017) port geographical locations place them at risk to disruptive adverse weather events, whether these be short-term adverse events, or the long-term sea rise effects attributed to climate change. Severe weather events include heat conditions, cyclones, flooding, bushfires, thunderstorms and tornadoes, water crises, storm surges and coastal erosion, and more recently, the onset of thunderstorm asthma syndrome which led to health issues and deaths in Melbourne (Schmidt-Thome 2006; Berle, Asbjørnslett, & Rice

2011; BOM 2017). Gharehgozli *et al*. (2017) describe these adverse weather events as 'wicked problems' which as discussed in Section 1.3 can be difficult to treat due to their complexity, open-ended and intractable natures. Further, recognition of hazards and risks within a wicked problem context appears to be rarely addressed by bureaucratic decision makers inclusive of port managers, either within the port's internal risk management processes, or within a wider, networked external stakeholder context (Roberts 2000; Head & Alford 2015; Gharehgozli *et al*. 2017). Individual hazards with relevance to Australian ports are now discussed in more detail, with relation to whether the hazards arise within the port, or externally as shown in Figure 3-3.

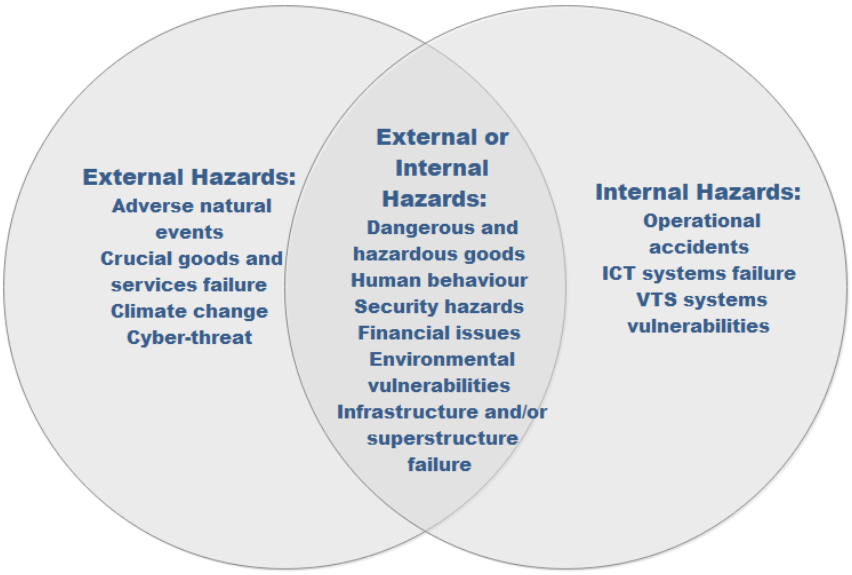


Figure 3-3: Origins of selected port hazards (Author).

3.5.1. External port hazards

Global trade throughput becomes more vulnerable to threats as it slows to pass through the port's land/sea interface (Bueno-Solano & Cedillo-Campos 2014; Stažnik, Babić & Bajor 2017). Ports experience multiple risks arising from within their managed areas and activities, and from outside designated port boundaries. External port hazards are largely beyond port management control; however, a full vulnerability assessment process requires port risk managers to develop understandings of their external risk environment, inclusive of stakeholder dependencies, connectivities and external actor vulnerabilities (Linkov & Palma-Oliveira 2016).

The impact of some external hazards may exceed port infrastructure design capabilities, or be beyond port management abilities to cope, either from the impact of one major hazard or the simultaneous effects of several small and seemingly unconnected hazards (Linkov & Palma-Oliveira 2016; Solecki, Pelling & Garschagen 2017). Port managers must either absorb the external risk shock and system degradation as best possible, or experience port operational failure and then undertake eventual reorganisation and recovery (Trump *et al.* 2016). The discussion begins with an investigation of external port hazards inclusive of adverse natural events.

3.5.1.1. Adverse natural events

Unlike other types of hazards, adverse natural events are argued to be becoming fewer, and increasingly severe in their consequences (WEF 2018). Adverse natural events can result in complex outcomes, as demonstrated by the 2011 Japanese tsunami and Fukushima nuclear power station meltdown, and consequent port radiation contamination (Wang, Cato & Shibasaki 2013). Severe weather events increasingly affect US ports (Gajjar, McLeod & Wakeman 2013). Superstorm Sandy impacted the US east coast in 2012, with 87 deaths and disruption to major ports and their supply chains (Burleson 2012; Wagner, Chhetri & Sturm 2014). Sandy was classified as a category one storm, which is relatively minor when compared with the category 4 and 5 cyclones that regularly impact on Australian ports.

An increasing number and severity of floods threaten Australian port infrastructure and shipping operations (Tracey 2011; Keim 2015). Cyclone Debbie floods in 2017 closed the Port of Brisbane, Port Alma and Bundaberg and heavily impacted Queensland ports' critical supporting infrastructure, their road and rail connectivity to their hinterlands, and crucial goods and services suppliers' assets and superstructure (Reynolds 2017). Severe natural events such as Queensland floods are described by the World Economic Forum as increasingly likely. Australian severe natural events from 2004-2017 (BOM 2017; CSIRO 2017) are shown in Figure 3-4, representing diverse levels of risk to ports and their hinterland stakeholders.

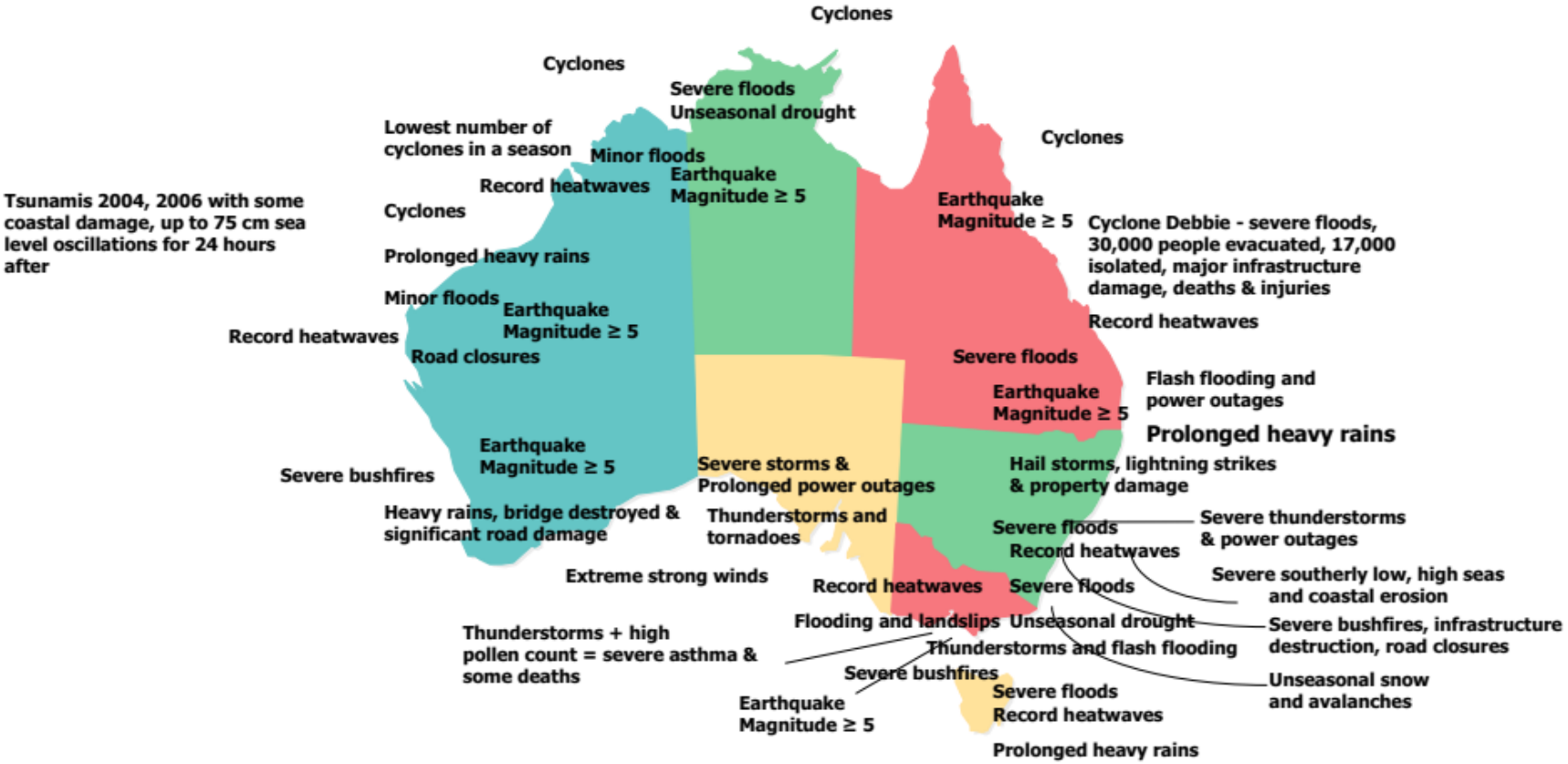


Figure 3-4: Geographic distribution of adverse natural events (Author, from BOM 2018 meteorological statistics).

3.5.1.2. Risk analyses for adverse natural events

Port risk assessment approaches for adverse natural events should make use of historical data, sometimes gathered over ten years, to fully evaluate the hazard and consequent port vulnerability. Port managers who conduct risk assessment should consider the potential range of losses including economic losses and conduct predictive modelling to better understand the data and improve the risk assessment process (Aven 2015; Dokic *et al.* 2016). Risk assessment (addressed more fully at Subsection 4.6.5.) incorporates the essential processes of risk identification and analysis, followed by risk treatment (Aven 2015). A simplified risk analysis model for adverse weather events is sourced from the literature and shown in Figure 3-5 to demonstrate some analysis features and decision support considerations involved in the risk assessment process.

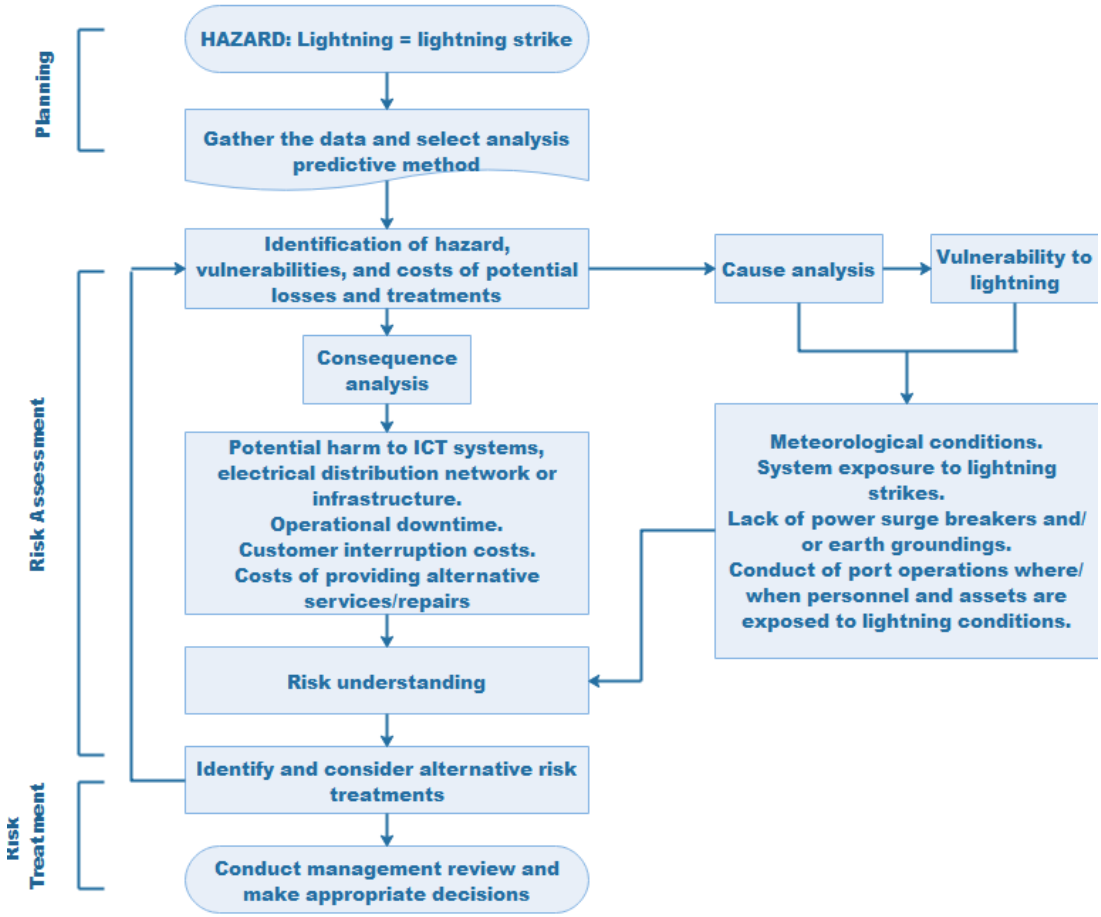


Figure 3-5: Risk analysis model (Adapted from Aven 2015, and Dokic et al. 2016).

While risk analysis for a lightning hazard is a seemingly simple process, a greater task arises in addressing the broader and more complex issues involving the potential failure of crucial external services providers (Loh & Thai 2014).

3.5.1.3. Crucial goods and services failure

The literature provides little guidance on how much regard port decision-makers apply to risks affecting their crucial external services and other port system sub-elements located outside port limits. The absence of this information provides a further layer of uncertainty to port risk analysis deliberations. Both the port and its external supporting networks of crucial goods and services suppliers are collectively exposed to known, unknown and unexpected sources of risk (Christopher & Holweg 2011). Whereas port managers might plan for and prepare to meet disruptions that might occur at the port, the port remains hostage to the vulnerabilities and uncertainties affecting its supporting networks (Power 2004).

This requires port managers to engage in external stakeholder risk management collaboration towards informational, planning and resource sharing purposes, within a regional and sometimes national context (Power 2004; Ponomarov & Holcomb 2009; Sloan 2009; Sakalayen, Chen & Cahoon 2017). According to Sloan (2009), implementing effective external stakeholder collaboration processes is a formidable and complex task, but important to port vulnerability because these crucial external goods and services suppliers comprise potential failure nodes for port operations (John *et al*. 2016).

3.5.1.4. Climate change

Climate change is well-researched from port and coastal community natural disaster perspectives (Gurning, Cahoon & Sambodho 2010; Nursey-Bray *et al*. 2012; Kong *et al.* 2012; Ng *et al.* 2013; Becker et al. 2015; Chhetri *et al.* 2015; Wakeman, Miller & Python 2015; Messner 2016). However, the rate of climate change onset to port operations is not a widely considered or well understood factor. Risks to port operations might manifest in the form of either subtle change with gradually worsening outcomes, or the impact of sudden change, for example the rapid onset of severe or catastrophic weather (Fritelli 2005). In the normal course of port operations, subtle adverse change might involve criminality or the development of a hostile or corrupt business environment (Rodriguez, Uhlenbruck & Eden 2002). In the context of climate change, ports might experience subtle

increases in climate-related risks over the next century (sea level rise and more severe storm events) with impacts varying from low to extreme (Maunsell 2007; Garnaut 2008).

There is little evidence that climate change threats figure greatly within Australian port risk assessments, possibly due to the slow nature of climate change - for example annual sea level rises of less than four millimetres per year (Garnaut 2008) likely represent a minimal threat within existing port manager tenures. However, US port studies indicate that an annual sea level rise of four millimetres per year represents a rate that requires early and costly elevation and protection of port infrastructure and fixed facilities (Becker *et al.* 2016; Becker, Hippe & Mclean 2017). Studies advocating that Australian ports should conduct climate vulnerability assessments and develop adaptation plans include Mullett and McEvoy (2011), Stenek *et al.* (2011), Ng *et al.* (2013a), and Becker *et al.* (2018). Australian port practitioners appear to be either unaware of the climate change discourse and recommendations or are disregarding climate change as a potential risk. However, Pachauri and Meyer (2014) argue that the impact of climate change is difficult for lay persons to detect - identification of an impact might require statistical testing, and the full consequences might take decades to fully unfold. It remains unclear whether port managers are motivated to introduce new mitigation measures in response to climate change, rather than maintaining existing natural disaster risk control and management measures.

3.5.1.5. Cyber-threats and port technology

Ports are increasingly reliant upon information and communications technology (ICT) in enabling connectivity, competitive advantage, effectiveness and efficiencies (Christopher 2011). Port ICT system usage includes electronic aids for operations and administration, security, navigation, record keeping, and real-time monitoring of systems. Other ICT usage incorporates weather stations, customer records, personnel management, communications within the port community, ship loading and unloading, materials handling and transportation, container movements, rail and crane operations. These factors are crucial to port operations

(Bichou, Bell & Evans 2014; Burns 2015; Bichou 2018) and should be addressed when evaluating port operational vulnerabilities (Coaffee & Clarke 2017). European research suggests that few ports conduct cyber-security vulnerability assessments (Beaumont 2017; Meyer-Larsen & Müller 2018) and the literature provides little information on these assessments within an Australian port context.

Ports likely have difficulty in coping with the rapid pace, complexities and hazards of technological change, digital innovation and associated risks of cyber-threats (Colarik 2006; Christou 2017; Nylén & Holmström 2015). This rapid pace of technological change and broadened hazard environment progresses faster than cyber-security abilities to respond, for example cyber threats mutate and assume new forms within just weeks (Ng 2017; Pleasance & Campbell 2017). The constantly changing forms and unexpectedness of cyber-attack upon global organisations constrain organisational abilities to perform normal tasks (Booth (2015). This ongoing contest between cyber-threat and cyber-security is exemplified by the WannaCry ransomware global cyber-attacks in May 2017, which were enabled by an infection vector called EternalBlue that was itself spread in April 2017 (Millar, Marshall & Cardon 2017). Organisations quickly implemented countermeasures to WannaCry, but between May and July 2017, two follow-on variations of WannaCry called Petya and Goldeneye were released with major impact on critical infrastructure including global ports (Ng 2017). Maersk port operations were impacted from 27 June to 10 July 2017 and incurred losses of US$300 million, showing how even global port leaders are underprepared to meet cyber-threats (Caldwell 2017; Dingledey 2017). Port resilience against the cyber-threat, according to Dingledey (2017) requires increased threat awareness and planning, staff training in security protocols, coupled with contingency and scenario planning, coupled with exercises and information sharing between organisations.

Port ICT challenges also include managing vulnerabilities to routine failures, human error, physical security, managing and keeping abreast of rapid advances in technology, protecting systems from the vagaries of weather, and the integrity of electrical supply (Lewis 2002; Onyeji, Bazilian & Bronk 2014). Essential port

operational services that are enabled by software systems become susceptible to unauthorised access, cyber-attack, user errors, and application code violations as shown in Table 3-3.

Port information and communications technology systems at risk of disruption	
Port management	Ship booking systems
Planning and scheduling	Road and rail traffic control systems
Ship and stockpile planning and scheduling	Ship loading systems
Demand planning	Radio frequency identification
Customer relation management	Cloud computing
VTS systems	CCTV management
Automated alarm systems (for land and sea)	Weather warning systems
Tsunami warning system	Swipe card access services
Telecommunications systems	Internet and intranet services

Table 3-3: A cross-section of port software at risk (Adapted from Ellison et al. 2010; Burns 2015).

The Australian Cyber Security Centre Report (2017) warns that organisations such as ports with extensive networks of critical goods and services suppliers are at risk of cyber-threats from incursions into third party ICT systems, which then transfer to the port systems. There is little evidence of Australian port managers being aware of this transactional technological risk.

3.5.1.6. Illegal immigration - consequences to port operations

Primarily the north-western Australian ports (Darwin, Derby Port Hedland and Broome) have experienced the consequences of involuntary migration with unannounced vessel arrivals and consequential port security and quarantine issues associated with 'boat people' immigrants (Phillips 2014). These vessel arrivals in Australian waters peaked during the financial year 2012-13 with 403 vessels carrying 25,596 passengers and crew (Phillips 2014). Uncontrolled and unexpected movement of vessels in port waters constitutes a safety problem for port vessel traffic management officers, particularly when these illicit arrivals interact with large, deep draught vessels that are restricted in their abilities to manoeuvre (IALA 2016).

3.5.2. Hazards arising from either external or internal origins

Some hazards might result from either internal or external risk causalities or contributing factors arising from within the port's internal processes and

procedures, or from external sources (Linkov & Palma-Oliveira 2017). An example is provided by logistics operations involving dangerous and hazardous goods.

3.5.2.1. Dangerous and hazardous goods

Australian port authorities, logistics entities and transport operators are responsible under State and national government Acts and Regulations for the safe handling, movement and storage of dangerous and hazardous goods (D&HG) within the port (AS:3846-2005). Cargoes within this category demonstrate explosive, flammable, toxic, infectious, spontaneously combustible, water reactive, corrosive, radio-active or pollutant properties (ADG 2017), for example crude oil, diesel and petroleum fuel, LNG, anhydrous ammonia, ammonium nitrate, and oxidising agents (House 2005). Cargo property uncertainties arise when:

a) liquid leaks or fumes involving unknown commodities emit from within cargo containers or packaging;
b) D&HG are stored in containers without declaration on the manifest; and
c) in the case of bulk heavy metals, dust release or seawater pollution occur during transportation or intermodal transfer (Bacchioni 2008; Alyami *et al.* 2014).

Further uncertainties and security risks related to containerised D&HG cargoes include smuggling, theft, or the possibility of non-manifested material intended for terrorism purposes (Bergin & Bateman 2005). Worst case containerised cargo scenarios include toxic or radiological devices that, upon initiation, would severely contaminate a large area through toxic, biological or radioactive release for short or long-term durations (Stern 1999; Cohen 2005). A single container incident offers potential for multiple risk consequences, for example shipping container accidents successively involving fire, explosion, and the release of toxic fumes or a hazardous liquid leak (Khan & Abbasi 1998; Pinto & Talley 2006). Much has been written about the accidental or deliberate use of ammonium nitrate as an explosive. Ammonium nitrate is extensively used for explosive purposes within the Australian mining resources industry, and explosive grade ammonium nitrate is

often mixed with dieseline just before use to create ammonium-nitrate-fuel-oil mix, abbreviated to ANFO (Zygmunt & Buczkowski 2007). This relatively common commodity is transported along port road, rail and sea corridors thereby posing a widely shared risk for multiple port-centric actors (Cassini 1998; Verm & Verta 2007; Ellis 2011).

3.5.2.2. Deliberate or unintentional human behaviour

Disruptions arising from human factors and behaviour are widely reported in the literature (Holmes 2002; Elias 2010; Fabiano et al. 2010; Wise, Hopkin & Garland 2010; Kaplan & Mikes 2012; Christopher 2015; Toscano 2016; Stranks 2016; Loh *et al.* 2017). Australian illegal substance abuse is reportedly increasing with an estimated 15.6% of Australians ($3.1 million) unlawfully using illicit and pharmaceutical drugs, primarily meth/amphetamines and pain-killers/opiates (AIHW 2017). This Australian study is based on 23,772 responses across a stratified, multistage random investigation encompassing paper, online and telephone surveys. Within the wider population, users are primarily young adults (Johnston *et al.* 2004; Stevenson 2004; Duff 2005; Frone 2006) with a growing trend for the misuse of prescription drugs (Lee & Ross 2011; Nicholas, Lee & Roche 2011). The hazards of working with dangerous and hazardous goods might be compounded by increased levels of workplace drug taking (WEF 2018). Research indicates that port workers using drugs might carry highly contagious infectious diseases through needle sharing, plus pose a risk to other workers while working under the influence of drugs (Cesar-Vaz *et al*. 2016). From a port workplace safety perspective, workers who are either intoxicated or affected by drugs must not be allowed near hazardous cargoes (House 2005).

Drug usage within the Australian workforce is predominantly by personnel aged between 20-49 (Pidd, Shtangey & Roche2008; AIHW 2017) however, and possibly related to workplace confidentiality restrictions, little is found in the literature about port employee drug taking. Australian drug users are predominantly male, employed, and arrange their drug habits to minimise detection by workplace safety screening processes, which increasingly reveal positive results for amphetamines (Duff 2005; Roche *et al.* 2008; Marques *et al.* 2014). Risk outcomes

from drug-taking (Duff 2005) include memory loss, depression, concentration loss, blackouts, moodiness and loss of concentration – underlying why workers either intoxicated or affected by drugs must not be allowed near hazardous cargoes (House 2005).

3.5.2.3. Security breaches

The Australian Maritime Transport and Offshore Facilities Act as amended in 2016 (MTOFSA 2003) requires Australian port authorities and all port and terminal operators to undertake maritime security functions related to intentional unlawful acts. This includes ensuring the safety of personnel, ships, infrastructure, cargo, plant and assets, and the IT integrity aspects of port and terminal operations. Additional port security concerns relate to adverse events or activities that threaten life, port operational capabilities, information and communications technology systems, cargo theft, data theft, criminality, vandalism, and sabotage (Manuj & Mentzer 2008; John *et al.* 2018). Rapid advances in the port use of digital technology also exposes the port to multiple aspects of cyber-crime (Accenture 2015). Vigilance is required against employee corruption by organised crime groups (Lantsman 2017) where trusted insiders at Australian ports might assist in smuggling activities or cargo theft. Criminal, terrorism or cyber-attacks that might arise from either within a port, or from external sources are described by Ekwell (2009, p. iii) as 'antagonistic threats against the transportation network'.

Increasingly, ICT technology advances make electronic business faster and provide companies with the ability and agility to create temporary and often anonymous online strategic alliances. The downside of these alliances is increased systemic complexity and uncertainty arising from:

a) real and virtual hinterland port stakeholder networks expansion;
b) a blurring of boundaries between what processes are physical and what are not;
c) not knowing where a company supporting the port is located; and

d) port support actors become increasingly further interrelated, interdependent and resultantly more vulnerable to 'domino effect' risk (Waidringer 1999; Tan, Lam & Zhang 2015).

Port physical security vulnerabilities are exacerbated by the port's typical location near metropolitan areas, uncontrolled and unprotected access by water, presence of dangerous and hazardous cargoes, and onsite storage of hydrocarbon products (Burns 2015; Christopher 2015). Diverse security challenges include social activist incursions and threats to operations; vandalism and sabotage; activist or criminal use of drone surveillance aircraft; organised crime penetration of the workforce; workplace violence; illegal substances and/or alcohol use by personnel onsite; and, people smuggling (Christopher 2015).

3.5.2.4. Financial issues

Australian port financial stress might arise as either a causal factor or a consequence related to cost overspend, fraud, theft, unsecure record keeping and storage safety, financial instability, banking transaction failure or business downturn (Shiller 2009; Pallis & De Langen 2010; John *et al*. 2015). Port authorities are not immune to employees' wrongful financial behaviour, for example corporate fraud (Lees 2017; Rintoul 2017). Flanagan (2008) notes that financial stress also arises from State government controls over port authority financial affairs, whereby Board independence might be influenced by Ministerial powers to appoint or dismiss government business agency directors and senior managers, to control strategic directions, and to shape corporate intent (Flanagan 2008; Whincop 2016). The relevant government department interacts with the port authority, for example as a regulator and adviser, and these interactions also empower the responsible Minister with governance powers beyond those contained in the Corporations Act (Whincop 2016).

Ministerial influence extends to the approval and control over how much port authorities might budget towards operational or capital expenditure, and what proportion of profits are paid to State revenue in the form of a dividend. This means that 75 - 95% of port authority annual profits might be passed to the port's

State government owner, with higher dividends required when State budgets experience financial stress (see for example, Western Australia State Budget 2017-18). These influences clearly reduce port authorities' ability to spend more on infrastructure replacement and maintenance.

3.5.2.5. Environmental issues

Australian port managers are required by their State governments to maintain environmental management plans, environmental management systems, and to conduct environmental monitoring processes. These formal plans are generally framed in accordance with ISO 14001:2015 Environmental Management Systems. Australian port compliance with these plans is mandated under its Environmental Protection Licences and its own master planning guidelines (Ports 2013). Environmental hazards associated with port operations include the transportation of dangerous and hazardous goods with potential risks including land, air and sea pollution, harm to the surrounding community, and harm to the health of port workers (Costa *et al*. 2017). Non-compliance with environmental regulations or codes of practice, or serious environmental pollution incident, can result in a regulatory authority directive to cease relevant port operations.

Port developments and some ongoing operational maintenance activities (for example dredging and sandblasting of wharf piles) require environmental assessments and impact statements. Port development projects are subject to socio-political risks ranging from community environmental concerns to more active interventions of anti-development groups and activists who might illegally enter port premises in efforts to halt port operations (Evans 2010; Connor 2012). Port-related environmental concerns include air pollution from ships, stevedoring, truck and rail motor exhausts, ballast water discharges, fuel and oil runoff into the water, cargo spillage or leakage, storm water runoff into the ocean, and, the storage and transport of industrial and ship domestic waste (Lam & Notteboom 2014; Burns 2015). Port environmental hazardous events include detection of marine invasive species (Bax *et al*. 2003); oil spills (Anderson, Melville & Jolley 2008; Hook *et al*. 2016); harmful effects of chemical oil dispersants (Hook *et al.*

2016); chemical spills (Storie 2014); impact on port of toxic fumes, smoke and runoff into sea from landfill fires and recycling depots (Fattal 2016); and, heavy metals contamination (Jones *et al.* 2005).

Flint *et al*. (2015) describe risks associated with ocean water quality at port areas:

a) agricultural and industrial run-off following heavy rains;
b) port, urban and coastal development storm water run-off;
c) vessel movements in port, dumping of rubbish, discharge of ballast water and anti-fouling paint chemicals;
d) seabed and plumes associated with maintenance and capital dredging, and rainwater or washdown runoff from wharf/loading facilities;
e) discharges, either managed emissions or incidents;
f) marine debris brought by tide or current from elsewhere; and,
g) commercial fishing, recreational fishing and boating, and shore-based recreation.

3.5.2.6. Infrastructure and/or superstructure failure

From a National Ports Strategy perspective (IA 2011, p. 6) '…ports and associated infrastructure are of the utmost economic and social importance to Australia'. In general, ports are regarded as particularly risk prone because of their infrastructure compactness, the typically extended replacement time and expense involved in replacing damaged equipment, the lack of redundancy should essential navigational channels become blocked, and hazards to life, environment and infrastructure associated with the throughput of dangerous and hazardous goods (Bichou, Bell & Evans 2007; Burns 2015; Bichou 2018). Some port risk studies refer to infrastructure and superstructure as if these are interchangeable terms. However, superstructure, plant and equipment are more complex and likely have a shorter life than infrastructure, and hence become potentially more susceptible to failure (Tsinker 2004, 2014; Bichou, Bell & Evans 2007; Burns 2015; Bichou 2018).

Additional to internal port infrastructure risks, ports are exposed to vulnerabilities affecting external infrastructure providers. While ports themselves constitute

compact centres of infrastructure (wharves, roads, rail, channels and support systems) the port infrastructure interdependencies with external agencies create external risk management considerations towards the continued availability of electricity, rail, road, water, fuel, ICT, health, airport, council and other critical infrastructure providers (AG 2011; AG 2017). The Australian government encourages public/private sector critical infrastructure providers to adopt organisational resilience as a key component of their risk management strategies (AG 2015; IA 2016).

Little is known about the effectiveness of Australian port critical infrastructure risk management and resilience interdependencies, for example the degree of infrastructure provider motivation, resources or opportunity to maintain or improve their risk management and resilience practices (Kwan & Balasubramanian 2003).

3.5.3. Internal hazards

Hazards arising from internal sources are possibly best understood by port managers, and in the case of organisations in general, evidence suggests that the majority have crisis management plans with a core element of preparedness towards internal risk consequences (Johansen, Aggerholm & Frandsen 2011). Port managers possibly find that risk assessments and risk level monitoring are easier to conduct when the hazards under investigation relate to their own port's internal operations (Loh & Thai 2014).

3.5.3.1. Operational port accidents

Accident analysis is broadly employed as a measure of port vulnerability to hazards (Darbra & Casal 2004; Grech, Horberry & Koester 2008; Lu & Tsai 2008; Yip 2008; Chlomoudis, Pallis & Tzannatos 2017). Within this context, Darbra and Casal (2004) review 471 major accidents across the ports of 95 countries from the United Kingdom's Major Hazard Incident Data Service data base (MHIDAS 2002). Major port-related accidents discovered by Darbra and Casal (2004) primarily related to fires and explosions, and accidents from all causes involved the following port operations:

a) transportation of goods in trucks, trains and ships;
b) cargo loading and unloading operations;
c) storage and process plant activities;
d) ship navigation in port – groundings, heavy impact with port infrastructure, and ship-ship collisions.

These accident causalities are revisited by Casal (2017) who finds that fire and explosive hazards continue to be of major concern to port risk evaluations, and that air and water pollution are likely secondary outcomes of such accidents. Casal (2017) argues that an initial step in establishing present organisational effectiveness in coping with disruption requires a historical analysis of previous risk management performance. From such an analysis, Casal (2017) discusses how the effects of an initial accident in port (even minor) might cascade across port infrastructure and activities to create further hazard scenarios, with worsened consequences. This 'domino effect' risk is exacerbated by the proliferation of dangerous and hazardous materials passing through port, either while being transported, handled or stored (Loh & Thai 2015; Fu, Wang & Yan 2016; Casal 2017). Port technology evolution has achieved such a high degree of automation across infrastructure, equipment and systems that in the event of information and communications technology (ICT) failure, port managers have utmost difficulty in adapting through manual interventions (Kramek 2013; Burns 2015; Beaumont 2017). ICT failure at a container terminal is a particularly daunting prospect because corruption and loss of the data base would result in inability to readily identify containers for release from storage; manual identification of containers could possibly take weeks during which port congestion occurs (Beaumont 2017).

Kramek (2013) highlights a requirement for port managers to undertake cyber-security assessments, produce cybersecurity response plans and to allocate funds towards ICT failure management. However, Beaumont (2017) assesses the literature related primarily to US and European ports and finds little evidence that port managers have taken up the Kramek (2013) recommendations. Brasingon and Park (2016) note that Australian ports have so far been minimally affected by

cyber-threats, however the level of port interactions with other industry ICT systems provides a degree of vulnerability from attacks affecting third parties. New insurance products are being established to cover 'crisis management forensics, security specialists, information and communication asset rectification costs, cyber business interruption costs and cyber extortion cover' (Brasington & Park 2016, p. 24).

3.5.3.2. VTS systems vulnerabilities

Vessel traffic services (VYS) support ship navigation operations through a complex matrix of reliable voice communications, automated information services, accurate navigational charts, real time tidal and meteorological information, hydrographical survey data, radar, CCTV, telephone, telex, facsimile, automated data transfer systems, and online recording and reporting systems (IALA 2016). Human inputs to port shipping operations require vessel traffic services officers overseeing navigational directions and communications with all vessel movements, monitoring of developing traffic situations, emergency management in accordance with Harbourmaster directions, and coordinating emergency communications (IALA 2016). If a crisis occurs while vessel movements are in progress, then reliance upon effective ICT systems assumes greater importance, with ship-shore risk management and safety communications becoming events-focused and reactive in managing evolving and uncertain circumstances (Seeger 2006; Glik 2007). Port operations are vulnerable to failure if VTS operators are deficient in monitoring, identifying and assessing risks associated with ship traffic, or are unclear about their assigned risk response actions (Jones & Preston 2010; Coombs 2015). VTS malfunction is also linked to the potential for cyber-threats and ICT system failures, as vessel traffic management and information services are provided from within the port's wider ICT system (Heilig & Voß 2017b).

Intentional or unintentional VTS failures can result through signal jamming, and if both ship and shore systems fail, then the outcomes can be serious. For example, the entire ship navigation is highly reliant upon the continued availability of the global positioning system (GPS) and if GPS inputs fail then the electronic chart

display and information system (ECDIS) will cease operating, multiple alarms will actuate or other linked navigation and communications systems, and ship navigations teams will risk loss of situational awareness and navigational safety (Grant et al. 2009). Tugs also rely on GPS for the same navigational system purposes, and the port authority VTS system is used for plotting ship movements, identifying vessels by use of the VHF automated identification system, and for safety communications purposes (Grant *et al*. 2009). GPS and VTS failures as two linked vulnerabilities constitute important hazards to ship and port user safety.

3.6. Summary

Australian port managers are challenged by hazards arising from within a dynamic and turbulent risk environment, and some hazards materialise in the form of new, unforeseen and unprecedented emerging risks. A closer understanding of risk-related terminology and clearer knowledge of the known types of port hazards and vulnerabilities are foundational to exploring port vulnerabilities and preparedness in meeting these hazards. The literature suggests that ports are increasingly vulnerable to extreme hydro-meteorological events, cyber-attacks, deliberate or unintentional human acts, and data theft or fraud. Port management effectiveness in treating risks from multiple sources is crucial, not only for the benefit of port users, but because the nation's industries and national economic prosperity rely heavily on ports maintaining their business continuity. Port managers must cope with multi-layered and multi-hazard risk environment challenges; however, little is known about Australian port managers' risk management capabilities, or of their training and competencies for making evidence-based judgements on risk. Risk management strategies and practices employed by port decision-makers in maintaining business continuity are discussed in the following Chapter.

Chapter 4: Port risk management strategies and practices

4.1. Introduction

The previous chapters provided an overview of Australian ports, the contexts in which they operate, and some categories of hazards that challenge port operational business continuity. However, this conceptualisation of the port and port hazards is unlikely to remain static. Ports and their operating processes, practices and crucial requirements are rapidly evolving and becoming increasingly complex, thereby expanding the risk environment. Externally, new hazards arise in the form of new, unpredictable and increasingly severe hazards of both natural and human causality. Port managers are at a decision-making crossroad, where they need to question the adequacy and effectiveness of their existing risk management strategies and capabilities against future risks.

The Australian Government (AG 2016) takes an increased interest in safeguarding national critical infrastructure systems (inclusive of ports) from disruption. However, Australian port risk management capabilities are an underexplored (if not unexplored) field of research. Consequently, little is known about how these ports manage risks and consequences associated with low probability/high consequence disruptions. Accordingly, Chapter 4 investigates the literature for evidence of port-oriented risk management knowledge, management capabilities and performance, and port operational business continuity performance. A capabilities-based vulnerability analysis model (originally a military concept) is examined for its notional suitability in identifying and assessing port systemic vulnerabilities (Schnaubelt, Larson and Boyer 2014). Further, a port risk maturity model is conceptualised as a performance and management capability measurement scale (Tarrant & Gibson 2010). Chapter 4 begins by tracing the origins of present day port risk management practices and processes.

4.2. Evolution of port risk management practices

The introduction of formal risk management practices to port operations can be traced to the mid-19th century (Brynjolfsson & McAfee 2014) when port safety,

design and environmental guidelines were introduced by PIANC, the Permanent International Association of Navigation Congresses (Van Der Burgt 1994). Formal risk management education began with the US Insurance Institute offering certification studies (Fraser & Simkins 2010). Formalisation of port risk management strategies, processes and techniques was furthered with publication of 21st century international risk management standards, including ISO 31000:2018 *Risk management -- Principles and guidelines.* ISO 31000:2018 is recommended by the Australian Government for departmental and business agency use, along with its companion document ISO/IEC Guide 73:2009, a risk management vocabulary (Knight 2009). Australian State Governments provide insurance cover for their non-privatised ports, and in reducing State exposure to risk, provide these State business agencies with risk management guidance and encouragement to adhere to ISO 31000:2018 methodologies and concepts (QLD 2017). The Australian government also encourages corporatised government business agencies (inclusive of ports) to adopt the resilience concepts within ISO 22316 *Security and resilience - Organizational resilience - Principles and attributes.*

The number of port-centric risk management and resilience standards extends far beyond ISO 31000:2018 and ISO 22316:2017 with primary supporting documents plus families of standards to encompass specific areas of operation, for example, IT security and environmental protection (ISO 2018). The number and variety of standards with applicability to port operations presents a complex challenge for port managers to understand what standards are crucial, and what might be occasionally useful. With the number of existing standards, plus multiple others under development for the management of risk, resilience and business continuity, port managers have more than thirty documents to consider as a basis for founding their strategies, plans, policies and routines (ISO 2018). Risk management and resilience learning is an essential component of port or other public-sector agency change processes, and decision-makers need to establish which core standards will suffice for organisational strategic and operational needs. Ports need to avoid management cognitive overland, where too much information might challenge port management's 'absorptive capacity, i.e. its

ability to recognize the value of external information, assimilate it, and apply it to productive ends (Piening 2013, p. 239). Alternatively, and from a social science perspective, Australian port authorities are predisposed towards a bureaucratic style of management (Everett 2007; Chen & Everett 2014) and a possibility exists that port managers could be reluctant to engage in new learnings and change. Aversion to change is a factor that could lead to port management reliance on a defined, long-established and narrow span of disruption management capabilities (Piening 2013). This possibility is a potential constraint to management critical thinking about the port's risks and vulnerabilities and runs counter to resilience concepts. Change in port risk management evolution is driven by port authority Boards of Directors in a top-down exercise of the control relationship between corporate governance and risk management (Robinson, Francis & Hurley 2013). Board governance and risk management understandings in turn are shaped by the international standards, plus the influences of professional guidance organisations, which for Australian ports include the Australian Institute of Company Directors (AICD 2016). Knight (2010, p. 16) for example, describes the role of corporate governance in furthering risk management as: 'the glue which holds the organisation together in pursuit of its objectives, while risk management provides the resilience'.

4.3. Port governance, risk control and corporate objectives

The linkages between port governance, risk, controls and corporate objectives vary from port to port in complex multiple aspects. Reasons for this variance relate to non-alignment of stakeholder self-interests, differing needs and interests, and elements of uncertainty and ignorance associated with the complexity of whichever risks affect each port (De Marchi 2015). Contemporary risk governance towards complex risks, according to De Marchi (2015, p. 162) requires managers and academics to recognise that such complexities exist, and to realise that risk complexities can be neither 'be fully understood nor managed with traditional risk assessment tools'. This section explores the literature to gain an overview of risk management from a port corporate objective perspective.

4.3.1. Internal and external risk governance

To optimise port business continuity outcomes, port risk managers should consider both internal and external risk governance (ISO 31000:2018). Ports have an opportunity to control their internal risks, but less ability for external organisations. External organisations of interest to ports include regional networks of stakeholders who provide the port with crucial goods, services, and other transport and logistics needs. The management of port systemic risks and vulnerabilities requires coordination and collaboration of effort across the networked port sectors, a process that requires robust risk governance mindsets and behaviour (IRGC 2015). Further, continuous monitoring of the port's internal and external risk environments assists in providing early warning of disruptions (IRGC 2015). Where risk governance instabilities exist, potential arises for adverse human intervention, for example terrorist, sabotage, criminality, activist or cyber-threat activities which are an increasing feature of 21st Century risk environments (Rubin 1998; John & Nwaoha 2016; WEF 2018; AG 2017). Risks of human causality add to a port's systemic operational complexities, vulnerabilities and uncertainties, and substantiate this thesis' focus upon a requirement for increasing port resilience (Coaffee & Clarke 2017).

4.3.2. Risk and uncertainty

Elements of port risk management uncertainty might arise from management ignorance of risk environment variables, cause and effect relationships, potential courses of action to take, and unknown potential consequences (Hillson 2005; Renn & Klinke 2015). Port lack of knowledge or information concerning risk might be described as *aleatory ignorance* (known unknowns), whereas uncertainties involve *epistemic ignorance* (unknown unknowns) or, as described by Hillson (2005, p. 5): '… risk is measurable uncertainty; uncertainty is unmeasurable risk'. In minimising uncertainty, an organisation might begin by aligning its risk management, corporate governance and strategy processes (Bromiley *et al.* 2015). Risk governance as a corporate process is necessarily guided by a cohesive framework for managing risks, uncertainty and complexity (Renn 2014). In past years, risk governance was based upon managers' experience with various

categories of risk (Mokhtari *et al*. 2012), which is a values-based rather than evidence-based perspective (Aven 2016) and which might have overlooked or ignored some categories of risk. An evidence based approach requires deeper knowledge of risks than port management intuitive or experience-led brainstorming sessions, as described in the port risk literature (Srikanth & Venkataraman 2013; Bichou, Bell & Evans 2014; Burns 2015).

Despite the physical and behavioural differences between ports, all are challenged by four primary categories of risk (Robinson, Francis & Hurley 2013; Hopkin 2017):

a) risks with negative consequences (pure risks);
b) uncertainties and unknowns (control risks);
c) legislative, regulatory or code of practice requirements for hazard management (compliance risks); and,
d) opportunities where potential consequences might result in either negative, status quo or positive outcomes (speculative risks).

From a port intermodal operations context, risk management's importance is attached to the three primary risk categories of pure risks, control risks, and compliance risks. Opportune risks, a fourth category, are regarded as less important to this thesis as they relate to potential benefits from risk-taking, which is peripheral to this research problem. In meeting these three important risk categories, port risk governance systems must encompass strategic and tactical planning, decision-making, and risk treatments aligned with the objective of achieving strategic and operational objectives (ISO 31000:2018; Lark 2015). According to Lark (2015), successful risk management implementation requires senior management to gain commitment to the risk management process from all personnel, in all departments, at all levels within the organisation. Corporate governance is conceptualised as a system of coordinated activities and accountabilities for regulating and overseeing enterprise-wide conduct, in which risk management becomes a key controlling mechanism in achieving corporate objectives (Dahms 2008; Lark 2015; du Plessis, Hargovan & Harris 2018).

4.3.3. Port risk governance

The function of port risk governance effectiveness is rarely investigated, despite the decisive role of risk governance in managing high consequence risks with potential to develop into system-wide critical infrastructure crises (Aven 2011). Organisations might base their risk governance and risk management processes on diverse approaches as described by Knight (2010) and Butterfield (2017):

a. traditional risk management (silo-based treatment of risk with little knowledge or consideration for whole-of-organisation risks);
b. enterprise risk management (a strategic, holistic risk approach to internal and external assets, resources and activities); or,
c. a superficial 'tick and flick' compliance-oriented approach just sufficiently detailed to satisfy auditors and regulators.

Risk governance establishes the direction and oversight requirements for all port risk management activities and is a process that begins at Board and senior executive level. A port risk governance framework is an integral subset of the port's wider corporate governance processes, and its objectives are to identify the resources to be used in managing risks, and to assist in effective decision-making and the establishment of risk management objectives (BS 31100:2011).

Gaining a specific understanding of Australian port capabilities and abilities to manage high consequence risks requires a multi-disciplinary investigation into technical, sociological and natural port hazards (Renn 2017), and establishing whether risk governance and risk management shortfalls exist against these broad hazard categories. Technical, sociological and natural hazards require individual risk management approaches, some of which might be incompatible with others (Renn 2017). The International Risk Governance Council (Florin & Bürkler 2017) provides a risk governance definition that reconciles so far as possible the limitations of a multi-disciplinary approach in exploring port risk. The IRGC (Florin & Bürkler 2017, pp 5-6) definition of risk governance is:

> The identification, assessment, management, evaluation and communication of risks in the context of plural values and distributed

> authority. It includes all important actors involved, considering their rules, conventions and processes. It is thus concerned with how relevant risk information is collected, analysed, understood and communicated, and how management decisions are taken and communicated.

This definition and the guidelines provided by the IRGC are important yardsticks for port Directors and senior managers in aligning risk governance within their overall corporate governance structure. Responsibilities for understanding and managing risks are vested firmly with an Australian port's Board of Directors, and the Directors are tasked with ensuring that port risks are managed and governed competently and effectively (AICD 2016). Whereas the Board might delegate accountability and authority for managing risks to managers, Directors cannot delegate their risk management responsibilities (Corporations Act 2001; Graham & Kaye 2015). Board responsibility includes resolving high level risk management conflicts, for example risk avoidance versus increasing profitability, establishing risk management priorities or validities, or authorising risk management budget funds (Schiller & Prpich 2014). Exercising such responsibilities requires a full and clear understanding of the port organisation and its risk vulnerabilities, a concept that mirrors the IRGC (2017) risk governance framework approach.

Risk governance frameworks are drafted by an organisation's Board and senior managers in response to two risk influences – compliance towards legislation, codes of practice or regulations, and, decision-making in response to perceived hazards, uncertainties and unknowns (Dahms 2008). Accordingly, while each port's risk governance framework might be unique, all should provide an effective control environment towards achieving corporate objectives, within acceptable risk limits (Dahms 2008). Corporate governance requires accountability and responsibility - Boards assign top down accountabilities and responsibilities to port risk managers who then perform bottom up risk management functions (Crowther & Seifi 2010; Robinson, Francis and Hurley 2013).

Port authority Board members sit on internal governance committees variously titled as: risk and audit committee, risk oversight committee, audit committee, or risk committee (Lam 2014). Risk management is a critical oversight responsibility

for Board members, inherent with their obligation to maintain adequate risk management systems under s912A(1)(h) of the *Corporations Act 2001* (Austlii 2018). Directors must remain cognisant of the nature and extent of risks that might challenge the port, and be confident that management is competent, capable and effective in their risk management roles (AICD 2016). These governance obligations require an understanding of how and why a port becomes vulnerable to the changing risk environment.

4.3.4. Vulnerability identification and assessment

As discussed in Chapter 2, port managers are challenged by new and emerging uncertainties, complexities and ambiguities that test vulnerabilities at each level of a port's operations (Gray 2017; Lam & Lassa 2017; Renn 2017). Seaport operational vulnerabilities are addressed in the literature but primarily from narrow approaches. For example, McEvoy *et al.* (2013) and Chhetri et al. (2015) take climate change approaches, while Pitilakis *et al.* (2016) investigates port vulnerability from a natural hazards perspective. Neither of these researchers provides a modelling framework that is applicable to port operational risk identification and vulnerability assessment. The military and security research fields provide examples of vulnerability modelling and simulation, primarily of a sophisticated quantitative format (Johansson & Hassel 2010; Wagner & Neshat 2010; Yang & Qu 2016; John *et al*. 2016, 2018). A semi-quantitative vulnerability assessment framework for practitioner use is proposed by Schnaubelt, Larson and Boyer (2014) from their work with military strategists. This framework appears to be readily adaptable and applicable to seaport vulnerability identification and assessment, and user-friendly for port managers with minimal access to sophisticated mathematical knowledge or software.

The Vulnerability Assessment Model (VAM) proposed by Schnaubelt, Larson and Boyer (2014) begins with identifying what actors, assets, resources and infrastructure are crucial to the port operations task. The second step is to identify crucial system requirements to maintain these primary support capabilities, and these crucial requirements form potential failure points (vulnerabilities) that need protection. Next, the process assesses:

a) which levels of vulnerability should be prioritised (for example, the top 10);
b) what risk management mitigation and response efforts should be allocated and where;
c) what business continuity strategies and plans should be implemented;
d) how these disruption response and management processes should be directed, and
e) how to design methods and capabilities for rapidly re-organising, modifying or adapting risk management processes as the situation demands (Schnaubelt, Larson & Boyer 2014).

From the literature, port capabilities critical to operational and logistics continuity consist of human resources, assets and infrastructure located within the port domain, which Trepte and Rice (2012) describe as the port's inner land and water area functional capabilities. Secondary capabilities (collectively integral to the port's effective logistical and transportation performance) are provided by the port's regional landside and waterside stakeholders and their port-centric assets, infrastructure and labour. Testing whether a port capability is critical to performance involves simulating what happens when that capability or its enabling requirement/s are removed – for example, if port cargo machinery requires mains electrical power and a disruption leads to power grid failure, then in the absence of alternative power supply, port cargo operations necessarily halt. Port resilience against this situation might involve having a standby emergency generator of sufficient capacity to replace mains supply for a given period. This Vulnerability Assessment Model approach appears to provide an evidence-based methodology (Aven 2016) for port vulnerability and assessment that strengthens the predominant values-based 'brainstorming' approach reportedly used by many port authorities within the past decade (Srikanth & Venkataraman 2013). Port decision-makers should gain the clearest understanding they can of the port risk environment and port vulnerabilities to hazards when formulating strategies and plans for controlling risk (ISO 31000:2009).

4.4. Understanding the port and port risk management practices

This section explores Australian port managers' understanding of their risk environment, their experience from past disruptions, and their knowledge of what categories of risks might manifest in the short-term future. Before a Board and their management team can design a risk management system, they must clearly and fully understand their organisation, its key dependencies and crucial requirements from both internal and external perspectives (ISO 31000:2018). They must also understand and be knowledgeable about risk and risk management (Hopkin 2017). Tarrant (2010) argues that effective risk treatment and effective disruption responses requires emergency team managers to be adequately knowledgeable and have all necessary resources quickly available. The management team should also be knowledgeable and practiced with the port's risk management policies, plans and operational priorities. Effective organisational risk management requires emergency response proficiencies, risk awareness and understanding, a sense of purpose and commitment to the task, personal and systemic capabilities, and a willingness to learn (Hopkin 2017).

Accordingly, port business continuity strategies and crises response plans should reflect accurate knowledge and understanding about all inputs and resources crucial to operational serviceability (Harrington 2015). Essential knowledge for risk management decision-making encompasses the port and its resources, its interrelated and interdependent actors and agencies, crucial support services, and the land/sea interrelationships and interdependencies between logistics and transportation processes. To maintain port business continuity in the event of disruption, managers must understand what alternatives are available in the event of losing the ability to use normal operating premises, and/or main supplies of electrical power, ICT services, road and rail transport, fuel, towage, pilotage, banking, potable water, waste removal, warehousing and storage (Bichou, Bell & Evans 2014; Burns 2015). Guidance for port disruption preparedness is typically contained in Australian State government emergency management plans (for example, TEMP 2015). A common requirement of these emergency preparedness and response plans is for responders to be practised in facilitating 'business as

usual' practices for as long as possible when disruption is imminent, and when required, to be capable of swiftly transitioning to their emergency management roles.

Zio (2016) argues that the quality and effectiveness of critical infrastructure risk management depends upon the strength of manager knowledge and experience. Additionally, Eggleston (2012, p. 85) argues that '… a healthy risk management environment is one where all members of an organisation are fully aware of the risks, controls and tasks for which they are accountable'. In practice, however, Eggleston (2012, p. 85) observes that non-compliance, inconsistencies, and indifference towards risk management stem from '…a lack of awareness, complacency, or no one person or group having responsibility or being accountable for their part in the process'.

The purpose of a top-down mandate and senior executive support for risk management (ISO 31000:2018) is intended to counter such mindset and behavioural shortfalls, but evidence from the literature suggests that this outcome is not always provided. For example, Tampubolon's (2012, p. 9) findings from a survey of Indonesian port managers' risk attitudes, awareness, and priorities (these survey findings utilise the abbreviation RM for 'risk management'):

> 'RM assessments only takes more time, money and energy'; 'there are many other business activities that require more attention'; 'RM approaches are not part of my job-desk, someone else was assigned for that'; 'my hands are tight-up (sic) cannot do more.'

Tampubolon (2012) findings that Indonesian port managers were unenthusiastic about administering risk management and safety functions are replicated to a lesser extent within the Kolář and Puckett (2011) survey of Australian, European Union and Canadian port authorities. Kolář and Puckett (2011) surveyed senior executives overseeing five large Australian container ports, using a survey questionnaire employing closed-ended Likert scale questions about management systems and governance. They find that two of five Australian senior port managers responding to their survey disagreed that port authorities should be

made responsible for port regulations, safety and security. These responses come despite Australian State government legislation requiring port authority Boards and management to undertake, as a primary responsibility, the organisational functions of risk and crises management – an example is provided in the Western Australia Department of Transport publication, *Port Authority Boards: Director's Handbook* (DoT-WA 2018). This finding (Kolář & Puckett 2011) suggests some evidence that senior port managers serving at two of Australia's twenty-seven port management have a less than total commitment to port authority risk governance. Port crisis management and business continuity are dependent upon strong risk management leadership and sound risk governance, and with weakened leadership commitment, a port might experience risk management failure (Clark 2016; Glendon, Clarke & McKenna 2016; Hillson & Murray-Webster 2017; Hopkin 2017).

4.4.1. Risk management failures

Extensive literature explains why risk management effectiveness is important, but less is known about why and how port risk management deficiencies might occur. Generic risk management failure is well researched with potential applicability to ports, and researcher findings are generally similar. For example, Stulz (2008) refers to enterprise communication failures in risk exposure knowledge sharing while Shefrin (2016a, 2016b) argues that risk management failures arise from a risk-taking organisation culture, errant human behaviour and mindsets, or through managers ignoring apparently inconceivable low probability risks. Bouvard and Lee (2016) contribute further causalities of risk management failure in terms of risk mismeasurement, ignorance, communications shortfalls, inadequate monitoring, risk management deficiencies, and employment of inappropriate risk metrics. Risk management failure according to Stulz (2008) originates from either one, or a combination of causes, including:

a) incorrectly chosen risk metrics;
b) incorrectly perceived 'known' risks;
c) overlooked 'known' risks;
d) deficiencies in internal risk information transfers; and,

e) risk register deficiencies in ongoing monitoring and management of risk.

Common features of these risk management failure studies include overlooking risks, incorrectly measuring risk, ignorance of crucial risk-related information, and risk management process deficiencies. Similarly, Leveson (2017) argues from a systems theory perspective that increasing levels of organisational complexity and resultant vulnerabilities constrain managers' ability to conceptualise their entire risk environment. Further, Renn (2017) suggests that risk identification is clouded by uncertainties and ambiguities, increasing organisational interconnectedness, and the fast pace of risk environment change – factors which in combination might exploit the previously described limitations of traditional risk management tools, and human inabilities to correctly interpret risk (Stulz 2008; Bouvard & Lee 2016). Leveson (2017) describes systemic complexities that might constrain risk decision-makers' abilities to identify and assess risks:

a) multi-layered and multi-sector interactions between many networked actors;
b) dynamic complexities arising as the system changes over time and adjusts to internal and external influences; and
c) complex non-linear interactions where risk outcomes seemingly have no obvious or logical relationship between cause and effect.

In the context of new and emerging risks, vulnerabilities arise when risk managers employ outdated risk mitigation towards new systems and technologies (Leveson 2017). Managers experience problems in mastering new technologies, coping with software failures, recovering from erroneous management decision-making, and in reshaping organisational culture to meet new risk mitigation and resilience challenges (Leveson 2017). Risk management failures also result from seemingly unjustifiable risk management costs, for example when a business case cannot be made for justifying expenditure upon inconceivable, low probability and high mitigation risks which are then ignored. An example is provided by the Fukishima nuclear power station melt-down, from which Tisdall (2013) reported on probabilistic risk assessment failures demonstrated by the power station

managers and their regulators. Tisdall (2013, np) records that managers upon reviewing their mistaken judgements observed that they should:

> Examine all the possibilities, no matter how small they are, and don't think any single counter-measure is fool proof. Think about all different kinds of small counter-measures, not just one big solution. There's not one single answer. We made a lot of excuses to ourselves… Looking back, seals on the doors, one little thing, could have saved everything.

Port susceptibility to risk management failure or a limited ability to cope with disruption might arise from similar governance and leadership causalities as those which led to serious disasters. Examples of notable risk management failures include the Three Mile nuclear accident, Bhopal gas leak, Challenger space shuttle explosion, Deepwater Horizon oil spill, Hurricane Katrina storms and flooding, and the Fukishima-Daiichi nuclear meltdown (Westrum 2006; Stulz 2008; Chernov & Sornette 2016). The global risk environment is altering, and new and emerging risks and compliance requirements will likely challenge port risk managers beyond their present levels of competence (Rubin 1998, 2004; WEF 2018). How port managers might respond to these dynamic risk environment challenges is unknown, as is whether their intended responses will correspond with the risk management and resilience competency findings within these literature review chapters.

Port risk management failure might also have its origins within the organisational tolerance to risk, if the Board of Directors sets their tolerance to risk at an unjustifiably high level, which Stulz (2008) categorises as a risk management trade-off between costs, innovative abilities and flexibility. If risks exist below a port's risk tolerance threshold and are ignored for this reason, then the port's risk monitoring may be challenged by what Stolz (p. 66) describes as the emergence of 'unobserved pockets of risk'.

4.5. Port tolerance and attitude to risk

Risk governance requires Board and senior management risk decision-makers to establish their organisation's attitude to risk, or risk tolerance profile and the

criteria by which risks will be identified and treated. Risk tolerance (or 'attitude') is described in the Orange Book as the amount of risk that an organisation is prepared to accept, tolerate, or be exposed to at any point in time (Treasury, 2004, p. 49), or as alternatively described, 'the organization's or stakeholders' readiness to bear the risk after risk treatment in order to achieve its objectives' (ISO Guide 73:2009, definition 3.7.1.3). In deciding how to treat a risk, port managers will likely decide whether the risk consequences exceed the risk threshold set within the organisational risk tolerance, and the probability of the risk event occurring. Port decision-making on how to treat a risk are based on determinations towards risk as paraphrased from Van Grinsven (2009):

a) accepting the risk on the understanding that either, internal controls are sufficient to mitigate the impact and consequences to an acceptable level, or that the probability of occurrence is deemed to be so low that the risk is ignored;
b) avoiding the risk through due diligence, alternative practices, or eliminating areas of risk that are not essential to corporate objectives;
c) transferring the risk, either to an alternative services provider or through insurance – noting that if risk transfer still leaves a port authority responsible for managing risk consequences, then this alternative loses validity; or
d) mitigating the risk, which is a common outcome.

Australian port authority risk tolerance is conceptualised as being conservative in nature, with evidence that these generally corporatised government trading agencies have bureaucratic management styles (Everett 2003b). So much so, according to Everett (2003a, 2003b) that port authorities' top-down traditional bureaucratic management frameworks result in cumbersome and rigid governance, operational and flexibility outcomes. A bureaucratic style of management has long been characterised as unsuited to coping with dynamic risk situations (Stacey 1993) because structurally, bureaucratic management styles follow strict Newtonian lines of cause and effect, predictability, and inflexibility. Rosenhead (1998) describes traditional bureaucratic thinking processes as

corporate 'tunnel-vision', while Burns and Stalker (1994) characterise bureaucratic management culture as being mechanistic, vertically controlled Weberian bureaucracy that operates within narrow and vertically integrated informational silos, wherein communications are processed at several levels before filtering upward to the executive level. In the port context a management silo is formed when the managers take only a narrow view of the organisation and matters affecting only their department and their functional areas (Mentzer 2001).

Pollitt and Bouckaert (2017, p. 72) argue that centralised bureaucracies in a Weberian configuration need to move away from their rigid structures and path dependencies and become '…more flexible, fast-moving, (and) performance-oriented' if they are to effectively manage contemporary rapidly-changing social, business and society environments. Port managers may be constrained in their abilities to be more flexible and react faster to rapidly changing situations because of staff shortages in specific areas. Christopher (2016) advises that if port managers are unable to keep pace with the changing risk environment, or require specialist expertise not held in-house, then external advisors, agencies or resources might be sourced on a needs basis. This thesis aims to test whether the outsourcing of risk management duties might raise potential difficulties in establishing and maintaining effective lines of control, communication and commitment with these non-employees.

The outsourcing of port staff duties also raises the possibility of behavioural bias occurring (Montibeller & Winterfeldt 2015) with non-employees struggling to understand the port risk environment and port risk governance processes (cognitive bias), and as non-employees either demonstrating lack of judgement in risk-related decision-making, or, not being fully committed to the port's risk management culture (motivational bias). Further behavioural bias issues in relation to a port bureaucratic mindset are discussed in the following section.

4.5.1. Behavioural bias and risk myopia

Organisations operating under a bureaucratic style of management aim for behavioural consistency with organisational goals and objectives (Kirsch 1997) and in addition to constraints in adjusting to fast changing risk situations (Stacey 1993)

a bureaucratic style of management becomes exposed to behavioural bias (Hrnjic, Reeb & Yeung 2015). Managerial myopia in relation to risk is a behavioural bias towards short term events rather than those occurring further into the future, and in the context of a rapidly changing risk environment, risk myopia and organisational tunnel-vision might constrain management abilities to identify new sources of risk (Booth 2015; Hrnjic, Reeb & Yeung 2015).

Contemporary hazards with low probability but extremely adverse risk consequences are difficult to predict due to their complex, unforeseeable and ambiguous nature and their often-rapid onset - for example: earthquakes, tsunamis, terrorist attacks, cyber-attack, technology failure, extreme weather events, economic and political turbulence, and human error (Weick & Sutcliffe 2007; Kobayashi 2013; Fiksel *et al.* 2015). Proactive decision-making regarding such hazards is impeded by a lack of knowledge, or management denial that low probability/high consequence categories of disruption will eventuate (Pate-Cornell 2012). Risk managers might subjectively regard unpredictable and unforeseen risks as deviations from their organisation's normal state of operational stability, and with a low probability of occurrence nebulous hazards become ignored (Aven 2015; Fiksel *et al.* 2015).

Criteria that further compound an organisation's inability to effectively manage risk include unanticipated complexity and behavioural factors at system level. The port-centric system creates a regionally dispersed operating environment whose actors may be unable to detect initial signs of unexpected system disruption or failure early enough to take decisive and effective countermeasures, and this coordination and visibility issue also constrains the effectiveness of multi-agency disruption responses (Haimes 2016; Salmon *et al*. 2011). Effectively, port risk management might be constrained by intentional or involuntary risk myopia.

4.6. Port risk management framework

Port risk management is practiced either formally or informally under many names and approaches (Lam 2014) and typically, port risk within the port governance context is regarded as adverse risk as opposed to private sector interest in both

adverse and opportune risks. When the Board directs management to implement 'top down' risk management instructions, the managers subsequently refer to a risk management framework in their 'bottom-up' engagement in risk management practice (ISO 31000:2018). A risk management framework constitutes a blueprint for managing risks, outlining what strategies, plans, processes and techniques are to be used (ISO 31000:2018). This framework should reflect best risk management practices but should not drill down into the risk processes to detail how risk treatment is performed. For example, COSO (2004) identifies an effective risk management framework as one constructed to:

a) minimise the possibility of gaps or shortcuts arising within the organisation's risk management practices and processes;
b) provide a more rigorous, even and consistent application of these risk management practices and processes across the organisation;
c) facilitate the formal inclusion and integration of risk management within all operational programs and management processes; and
d) provide a proforma structure for managing new and emerging unexpected risks within an increasingly complex and turbulent risk environment.

Different levels of risk management exist within a port organisation because port authority operations are supported by multiple processes that are overseen by differing management levels within separate departments. Each management group has different perspectives on risk as it affects them, and individual managers are necessarily mindful of varying types of risks (BS 31100:2011). Strategic directions for risk are set by the Board of Directors and senior managers, the strategic directions are converted into plans, programs and processes by middle management, and operational risk management and disruption management processes are implemented by these middle level managers and frontline employees (BS 31100:2011; Loh & Thai 2015). The differing risk management processes that occur at varying levels within the port organisation are typically reflected in its risk management framework (Loh & Thai 2015).

Australian State governments provide guidelines for departmental risk management frameworks, but port authorities as corporatised business agencies

operate outside the direct control of their State government, and do not have to comply with State government directions. Instead the port authorities are *encouraged* by State governments to implement a framework that is consistent with the *AS/NZS ISO 31000:2018 Risk Management Principles and Guidelines.* Standardised risk management methodologies and approaches within these guidelines are typically constructed around a P (Plan), D (Do), C (Check) and A (Act) framework (Reason 2016). The predecessor to this standard was AS 4360:2004 which was published in 1995 as the first global standard in formalising and standardising risk management practices (Knight 2002). ISO 31000:2018 recognises that risk needs to be managed either in the aggregate across the organisation, or within specific areas of 'strategies and decisions, operations, processes, functions, projects, products, services and assets' (ISO 31000:2018, p. 1). The standard addresses how risk and risk management affect an organisation's objectives, which in this study, relates to port operations and specifically, the port's ongoing objective to maintain continuity of its two-way intermodal transfers of cargo and passengers.

Port managers have access to multiple standards, codes and practices that assist them in compiling and implementing strategies, policies, plans and procedures to achieve their core operational objectives. Kouns and Minoli (2010) list seven international risk management standards that apply to information technology security alone, and a possibility exists that having too many guidelines might create confusion, and difficulty may arise in establishing what managers need to know, versus that which is 'nice to know'. Other examples of risk management frameworks are contained in:

a) AS/NZS 4360:2004 Australian and New Zealand Risk Management Standard;
b) COSO (2013), Enterprise Risk Management – Integrated Framework;
c) The Orange Book – 'Management of Risk: Principles and Concepts' – HM Treasury (2004) (UK); and,
d) Integrated Risk Management Framework (Canadian Treasury Board, 2000).

The UK Orange Book and the Canadian Integrated Risk Management Framework are written for government departments and agencies, whereas the other three are written for generic organisations. Drafting of a risk management framework requires cognisance of multiple factors, including relevant legislation, codes of practice and regulations, and the organisation's risk policy created by the Board of Directors and senior managers (Dahms 2008). Australian port organisations have no fixed requirement for which risk management framework to adopt, although State governments encourage their government business agencies to adhere to ISO 31000:2018. As shown in Table 4-1, the ISO 31000:2018 risk management framework has shortfalls in areas that are addressed by other standards, codes and practices. These other risk management frameworks also have varying areas of weakness (Hopkin 2017), and so the remainder of this chapter explores port risk management strategies, plans and techniques against an ISO 31000:2018 framework.

Framework key features	**ISO 31000**	**AS/NZS 4360**	**COSO (2013)**	**Orange Book**	**IRMF (2016)**
Risk management required at all levels (strategic, tactical and operational)	✓	✓	✓	✓	✓
Clearly articulated risk management policy	✓	✓	✓	✓	✓
Specific risks cannot be addressed in isolation				✓	
Top down mandate for risk management	✓	✓	✓	✓	✓
Risk management at all levels, in all processes	✓	✓	✓	✓	✓
Reduce risk reliance on silo management			✓		✓
Risk focus on events (loss)		✓	✓	✓	✓
Risk focus on effects (positive or negative)	✓	✓		✓	
Acknowledges subjectivity, limitations			✓	✓	
Addresses information technology security			✓		✓
Clear lines of accountability	✓	✓	✓		✓
Reliance on internal risk controls and audits			✓	✓	✓
Understand the business	✓				✓
Need for effective risk communications	✓	✓		✓	✓
Ongoing review and continual improvement of risk management framework		✓	✓	✓	✓
Provides framework template/s	✓	✓	✓		
Emphasis towards public sector risk				✓	✓

Table 4-1: A comparison of integrated risk management frameworks under five international risk management systems (Author).

A simple risk management framework is compiled from ISO 31000:2018 and is shown in Figure 4-1 to demonstrate how risk is addressed at differing levels of the port organisation.

Figure 4-1: A conceptual port risk management framework (Adapted from ISO 31000:2018).

The framework begins with a top-down review of risks and a setting of risk management directions, tolerance and policies. These top-level decisions are translated into accountabilities, implementation plans and the establishment of requisite budget and resources to integrate and apply the chosen risk management practices and techniques into all facets of port operations (Giannakis & Papadopoulos 2016; Hopkin 2017). Risk management frameworks provide a methodology for identifying and assessing multiple risk exposures and for implementing and managing these risk exposures within an integrated framework rather than employing a silo risk management approach (Harrington, Niehaus & Risko 2011). This aspect of treating risk is discussed in the following section.

4.6.1. Integrated risk management/Enterprise risk management processes

Enterprise risk management is described by the *Committee of Sponsoring Organizations of the Treadway Commission* (COSO 2004, p. 4) as:

> A process, effected by an entity's board of directors, management and other personnel, applied in strategy setting and across the enterprise, designed to identify potential events that may affect the entity, and manage risks to be within its risk appetite, to provide reasonable assurance regarding the achievement of entity objectives.

Like traditional risk management, enterprise risk management (ERM) also has its critics. Power (2007, 2009) argues that ERM flaws include setting a single enterprise-wide level of risk tolerance whereas different departments might have differing exposure and appetite for risk. Power suggest that ERM flaws might be rectified by incorporating aspects of business continuity management within the organisation's risk management approaches, because business continuity management has similar aims to ERM but more focused techniques in keeping operations functioning in the event of disaster.

Critics such as Power (2009) and Hubbard (2009) argue that quantitative risk management processes, for example Monte Carlo simulations or other quantitative risk management software solutions, are potentially more effective than traditional or ERM processes on their own. However, not all Australian port authorities are large enough or financially capable of employing a full time Chief Risk Officer who is qualified and capable of performing quantitative risk analyses. Further, the benefits of ERM are only maximised if the port's risk governance and commitment to risk management are adequate and effective (Sadgrove 2016).

The objective of ERM is to increase an organisation's capability for proactively and strategically managing multiple risks on an integrated and holistic basis (Liebenberg & Hoyt 2003; Sobel & Reding 2004; Anderson 2006; Lam 2014). ERM processes share attributes of traditional risk management but ERM differs in amalgamating all risk management processes within a common framework, rather than silo-based treatment of individual risks treated in isolation by each department (Gatzert & Martin 2015). The value of ERM to port managers is outlined by Fraser and Simkins (2010) who describe ERM as a process that:

a) identifies potential hazard events that threaten the entity;

b) enables managers to operationalise and strategise risk within the entity's risk tolerance; and,
c) provides assurance that risk management outcomes will optimise the overall effectiveness and efficiencies of entity objectives.

With ERM, organisational risks are identified, assessed and monitored in a holistic manner, and risks are evaluated for both their individual and adverse interactive effects upon business continuity (Brustbauer 2016). Risks are prioritised so that maximum risk treatment effort is accorded to risks with greatest adverse impact upon corporate objectives. The term 'enterprise' describes either real or virtual systems, for example the port's regional network of goods and services providers (real), and the (virtual) cloud computing and ICT systems (Roberts 2006; Haimes *et al*. 2015). Ports are complex enterprises consisting of multiple actors and their communications platforms, plus external stakeholders and their interdependencies with the port (Mostashari *et al.* 2011). Traditional risk management processes are potentially challenged by the port's levels of complexity and its exposure to the uncertainties, unexpectedness and unknowns of the logistics and transportation risk environment (Weick & Sutcliffe 2015; de Martino *et al*. 2013).

Brooks, Fraser and Simkins (2010) suggest that an organisation aiming to cope effectively against uncertain and unexpected sources of disruption requires risk management defence-in-depth through:

a) visualising the increasingly complex critical infrastructure system that provides crucial regional support to the port;
b) recognising regional hazards and risk dispersion across the port's hinterland and foreland areas;
c) recognising the identities of crucial goods and services suppliers; and,
d) identifying and assessing risks challenging these crucial goods and services suppliers.

ERM is better placed than traditional risk management for understanding which port actors are vulnerable to systemic hazards, how individual actors and clusters of actors within the port community might respond to disruptive events, and how

port actor failure might affect the wider pool of stakeholders reliant upon port business continuity (Becker, Fischer & Matson 2013). Conceptualisation of the interactive, multi-directional and repetitive processes of enterprise risk management (Hopkins 2012) is aided by reference to a 3D integrated enterprise risk management framework model provided by the US CPA peak body (COSO 2004) as shown in Figure 4-2. The top surface of the cube represents four categories of objectives (strategic, operational, reporting and compliance); the front of the cube shows seven steps in treating risks from the internal environment (the same process holds true for treating external risks); and, the right side of the cube shows the organisation broken down into its integral units.

This COSO integrated enterprise risk management framework is described as the foremost global risk management standard (Tekathen & Dechow 2013; Hayne & Free 2014; Decaux 2015). However, Australian port managers are encouraged by their State government owners to utilise the ISO 31000:2018 risk management framework. A comparison of COSO ERM with ISO 31000:2018 ERM reveals that:

a. COSO ERM is much longer than ISO 31000;
b. COSO ERM consists of 120 principles versus 15 for ISO 31000;
c. COSO ERM was written by the accounting profession predominantly for the accounting profession, whereas ISO 31000 was written by multiple risk professionals for generic risk practitioners;
d. COSO ERM overlooks the importance of external stakeholders to the organisational business continuity task; and,
e. COSO ERM appears to be more focused on the auditor perspective rather than that of a risk manager (IIA 2012).

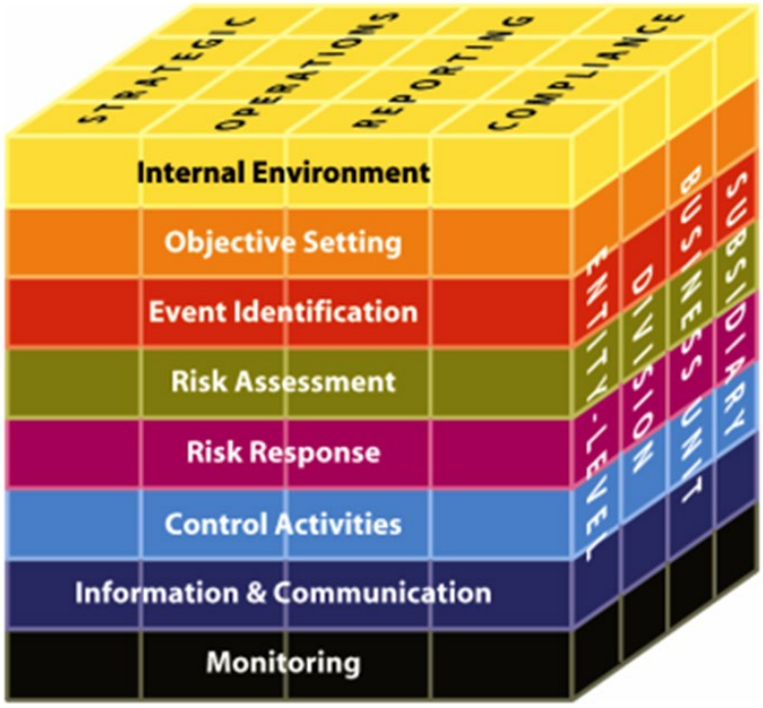


Figure 4-2: The enterprise risk management three-dimensional matrix (COSO, 2004, p. 23).

Australian port authorities are small to medium sized enterprises, with few employing more than 200 staff and in total these port authorities employ less than 3,000 full time employees (Ports 2016). The cost, resources, commitment and capabilities required to adopt, implement and comply with the COSO ERM system might be beyond port authority means, whereas the ISO 31000:2018 standard is simpler to use and less expensive to implement and audit (Dias 2017).

4.6.2. Traditional as opposed to enterprise risk management

Port risk management approaches, like those of organisations in general, have altered over the years to become more sophisticated, more widely focused, and more adaptive to rapidly changing circumstances (Fraser & Simkins 2016; Hopkin 2017). One marked change involves the transition from traditional silo-approach techniques to holistic enterprise risk management (Hopkin 2017). This development was influenced by realisations that silo approaches impede integration and coordination of risk management effort across the organisation (Hoyt & Liebenberg 2011). The changing nature of the risk environment has resulted in a wider range of port vulnerabilities to unconventional risks, and in addressing these vulnerabilities, holistic efforts are better suited for understanding and coping with complex and emerging risks (Rosenthal, Boin, &

Comfort 2001; Hopkin 2017; Renn 2017). Holistic risk management approaches have become necessary because of capability gaps in silo risk management approaches (Bugalla & Narvaez 2014; Paté-Cornell & Cox 2014) involving:

a) risk treatment efforts becoming duplicated;
b) underestimating the type and consequences of potential risks;
c) limiting the scope of risk assessments (particularly concerning low probability/extreme consequence events);
d) overlooking near-misses;
e) reduced recognition of the full effects of risk impact and consequences upon the organisation;
f) interactions between critical risks not being recognised;
g) crucial risk information not being shared, with ramifications for risks that affect multiple departments; and
h) senior management difficulties in conceptualising the organisation's aggregate key risks.

Traditional risk management is a highly disaggregated form of risk management, one in which the various categories of organisational risk are individually managed in separate risk silos (Fraser & Simkin 2011). Managers endeavour to understand the behaviour of each risk under nominal organisational oversight, and with minimal consideration for how a specific risk might affect other departments or the wider organisation (Fraser & Simkin 2011; Hopkin 2017). Managing risks in individual silos might make sense to some port departments, where for example the finance department could specialise in and become a centre of excellence for managing financial risks, while staff outside of the ICT department may not have sufficient expertise to manage cyber-risks (Bugalla & Narvaez 2014). However, within these management silos, staff become focused upon recognising and preparing for known risks, rather than low probability risks characterised by uncertainties, ambiguities and complexity (Chapman, Ward & Harwood 2006). There is still a role for silo risk management, when a focused and phased examination of disruption sources in a silo approach becomes useful for port

managers when they wish to identify operational vulnerabilities to specific risks and allocate appropriate risk treatments (Kleindorfer & Saad 2005).

Integrated and coordinated risk management efforts are key benefits of enterprise risk management frameworks, which have potential for higher quality of systemic risk governance and control that traditional risk management approaches (ISO 31000:2018; Fraser & Simkins 2016; Hopkin 2017). Ports have evolved from being singe intermodal actors to crucial elements of global supply chains (Robinson 2002; Wilmsmeier, Monios & Pérez 2013). Port integrations into landside logistics and transportation networks results in ports becoming individual complex adaptive systems within supply chain systems of systems (Cetin & Cerit 2010a, 2010b; Vonck & Notteboom 2016). Managing risk as a port system with crucial hinterland interrelationships and interdependencies is a greater challenge than managing risk as an individual entity, and seemingly a task beyond the capacity of traditional risk management. Yet Fraser and Simkin (2016) find from surveys within a US context that only 25% of large organisations report having enterprise-wide risk management capabilities in place. Studies that explore Australian port risk management capabilities from a systemic perspective appear to be negligible, except for research that addresses seaport climate change hazards (McEvoy *et al.* 2015; Cahoon *et al.* 2016; Becker *et al*. 2018).

Critical infrastructure, inclusive of ports, is necessarily a system of systems, comprised of many actors and multiple layers of interconnected and interdependent networks, mutually reliant on system members for continuity in their supply of goods and services (Pye & Warren 2007; IA 2016; AG 2017). Critical infrastructure network interrelationships and interdependencies render all participants of such a system vulnerable to hazards affecting one or more of their network members, through the cascading nature of disruptions (Hartwich 2012). The port shares fundamental attributes of network risk with other organisations within the critical infrastructure networks: complexity in risk causes and consequences; uncertainty involving organisational ignorance, interrelationship variability, and random variables; and, ambiguity regarding organisational interpretation of risk/s and normative behaviour (Renn 2008). Coping with

complexity, uncertainty and ambiguity is possibly a step beyond the capabilities of traditional risk management and its linear cause and effect approach (Smith & Irwin 2006).

Treating network risks is a potential problem for port authority bureaucratic management styles (Everett 2003; Pollit & Bouckaert 2017) because an uncertain and dynamic risk environment requires the exercise of flexible, adaptive and innovative management capabilities (Taneja *et al.* 2010). Traditional risk management suffers from inflexibility, whereby managers tend to '…recycle old solutions to new problems' (Moynihan 2008, p. 351). Consequently, port managers might look for more than what traditional risk management offers. An increasingly used, more versatile alternative to traditional risk management is the enterprise risk management approach (Fraser & Simkins 2010).

4.6.3. Risk management documentation

Port risk management practice is initiated by the Board in the form of a port risk management policy. Hopkin (2017) describes this initial step as crucial because it sets risk management within the required context and demonstrates Board and senior executive advocacy and commitment to enterprise-wide risk management strategies and processes.

Hopkin (2017) describes how the risk management documentation of each organisation will vary in relation to risk tolerance, the level of risk treatment required, and the complexity of the task. Additionally, the risk management documentation will reflect the Board mandate and follow a risk management framework in listing accountabilities, responsibilities, strategies, policies, procedures, plans and processes (Hopkin 2017). Other factors and practices detailed with a risk management strategy include organisation, risk prioritisation and monitoring, training and exercises, and budgeting towards allocation of risk management resources. Risk management documentation, processes and procedures must also address regulatory compliance needs

4.6.4. Normative risk management

Australian Government entities (including port authorities) must comply with the Australian National Disaster Resilience Framework (AG 2011), and this national emergency framework follows a normative risk management strategy of *prevention, preparedness, response and recovery* – a comprehensive disruption response mechanism termed PPRR (Cronstedt 2002; Rogers 2011). PPRR is employed as a foundational basis for constructing State-wide and local resilience capabilities (Cavallo 2014; Jenkins 2015). PPRR attributes are described by Linnenluecke and Griffiths (2013, p. 389) as:

> Disaster risk detection and preparedness planning including the identification, forecasting, mitigation, and avoidance of disaster situations (and) the analysis of community vulnerability (plus) strategies for effective emergency management and disaster response, and the mitigation of risk and losses.

National and international commercial, government and community organisations, inclusive of port managers, employ the PPRR risk management processes (Sujanto *et al.* 2008; Rogers 2011). PPRR is acknowledged to be a sound reactive risk management tool but reportedly its processes require modification to become more complete and proactive (Cronstedt 2002; Rogers 2011). Rogers (2011) indicates that PPRR processes benefit business continuity through their flexibility, innovation and adaption strategies; however, PPRR pays scant regard towards hazard awareness or monitoring for the onset of major hazards (Rogers 2011). These capability gaps lead to inability for early recognition of an incipient adverse event (organisational mindfulness) which is a key platform of organisational resilience (Weick & Sutcliffe 2015).

PPRR is unsuited to systemic risk management (Rogers 2011; McLaughlin & Fearon 2013) involving requirements for collaboration and coordination with the port's external system of interrelated and interdependent actors and agencies (Notteboom & Rodrigue 2005; De Martino, Morvillo & Marasco 2010). For example, some port-centric actors might choose not to act at all in response to a disruption, and rather adopt a 'wait and see' approach towards rapidly changing

events (McLaughlin & Fearon 2013). Maintaining risk management visibility over such a system is a daunting task, for example when attempting to identify which actors are actively involved at any one time and crucial to current port operations. Impediments such as these constrain a comprehensive port disruption response along PPRR lines (Rogers 2011), and further, port emergency response managers are required by legislation to defer to their local emergency management organisation when an incident controller is appointed by the State government to manage an emergency (OEM 2005; AG 2018).

For Australian ports, other than for undertaking their roles in the national emergency framework, there is little evidence to gauge the extent that PPRR concepts are otherwise employed, or the effectiveness of port PPRR response capabilities in managing disruptions. This lends importance to empirical investigation of port effectiveness in managing major hazards and associated disruption consequences, which is an objective of this thesis.

4.6.5. Risk assessment techniques and technology

ISO 31010:2009 Risk Management - Risk Assessment Techniques (a companion standard to ISO 31000) advises that risk assessments can be performed by qualitative, semi quantitative or quantitative techniques, or a combination of these techniques. Probity requirements for risk assessment, according to ISO 31010, are that the technique/s used for risk assessment should be justifiable, appropriate to context, productive of results that enhance risk understandings, and as with good research methods, should be 'traceable, repeatable and verifiable' (ISO 31010:2009, p. 18).

Researchers undertake scientific investigations of organisational risk management processes and techniques, and report on risk management techniques employed by organisations inclusive of ports. This aspect of port risk management is what underpins evidence-based risk identification and assessment (Aven 2016). The complementary component to evidence-based risk identification and assessment is a value-based process that relies upon management risk experiences and judgement (Aven 2016). Value-based processes rely upon qualitative and semi-qualitative techniques include brainstorming, mind-mapping, hazard matrices, risk

matrices, risk graphs, Delphi concept, scenario analysis and SWOT analysis (Berg 2010). Quantitative evidence-based risk management techniques are increasingly used in academic risk management investigations, for example Gurning (2011) and John *et al*. (2016) employ Bayesian techniques in better understanding the uncertainties of maritime risk assessments. Bayesian techniques include Markov Chain Monte Carlo simulation as used by Hubbard (2009) in practitioner risk consultancy, and Paté-Cornell *et al.* (2017) in a critical infrastructure cyber-risk assessment. John *et al*. (2014) employ an integrated fuzzy set theory risk assessment of port operations, and later propose (2015) wider use of fuzzy set theory coupled with evidential reasoning (Dempster-Shafer theory of evidence) in investigations of seaport risk management and decision-making under conditions of uncertainty. From a practitioner perspective, port managers may not have the specialist training and skills to engage in the statistical evaluation of risks, however in addition to port managers' access to Excel-based statistical capabilities, multiple user-friendly software packages and associated training are commercially available to assist port managers in their risk management and monitoring roles (Weeserik & Spruit 2018).

Patterson (2015) notes that the rapid evolution in risk management technology provides managers with increased capabilities to identify, process and manage risk-oriented data. Computer-based technology is also described as decision support systems and in the case of risk management, decision support systems assist in providing interactive information gathering and provision, thereby assisting decision-making procedures (Power 2007; Beroggi & Wallace 2012; Hollnagel, Leveson & Woods 2012). Risk management software is increasingly user friendly and flexible (Thoits 2009; Hopkin 2017), however difficulty arises for port risk managers when modelling port safety for auditing, competitive, or predictive purposes. This is because the literature contains largely mathematical models against which a port might be benchmarked, and mathematical modelling (for example John *et al.,* 2015 and use of fuzzy set theory) is more likely to be within the specialist risk manager province than with mainstream port managers.

An evaluation of Australian port authorities' organisation charts shown on their web sites indicates that few qualified chief risk officers (CRO) or equivalent managers work for the ports. Where a CRO is employed at a port authority, possibilities arise for the use of in-house software-based risk analysis and management packages to assist in:

a) compiling information on internal and external risk-oriented events and activities;
b) provide high level oversight of organisational risk status;
c) maintaining real time overview and awareness of factors affecting operations;
d) risk analyses;
e) measurement of organisational hazards and risk against desired objectives;
f) prepare general or specific reports on demand; and
g) maintaining risk, incident, and compliance registers (Thoits 2009).

Board level risk decision-making can be assisted by CRO advice and use of the CRO to funnel Board risk management advocacy is another way to garner organisation-wide commitment to risk management (Weeserik & Spruit 2018). In organisations without a CRO, the Board might delegate the senior management risk management responsibilities to either the Chief Executive Officer, Chief Financial Officer or Chief Operations Officer (Weeserik & Spruit 2018). What is not known is the extent to which these other senior port executives are qualified in risk management knowledge and skills, either from formal education or in-house training, and how risk education or its absence might affect port risk management capabilities and capacities. On-the-job experience and workplace training is necessary for the full development of port management skills, but further competency would likely result from a formal education foundation to provide technical skills (Manuti *et al.* 2015) is necessary for the full development of port management skills, but further competency would likely result from a formal education foundation to provide technical skills (Manuti *et al.* 2015).

Thoits (2009) surveys predominantly US organisations across multiple industries to obtain information on what tools these organisations employ to manage risk.

Of 651 respondents, 27% developed their own solutions internally, using commonly available desktop software including Microsoft Excel, Word, PowerPoint and Access; Lotus Notes; and Microsoft SharePoint (Thoits 2009). Five percent implemented custom developed software either in-house or from externally developed projects, while twenty percent employed specialised software to address specific functions within their risk management programs. A review of online product descriptions for risk management software indicates that multiple specialised software packages are constructed around either ISO 31000: 2009 or COSO enterprise risk management frameworks. These can be expensive, with an annual fee plus establishment costs, but port managers also have access to open-source risk management software that is provided free of purchase and annual costs.

It is unclear how applicable or relevant risk decision support systems might be to Australian port business continuity, whether port management teams have the expertise to employ quantitative risk management techniques, or whether quantitative techniques and software are of practical use in assisting port managers to cope with risk.

4.6.6. Risk mindfulness

Recent disaster and stressor events (for example terrorism, severe weather events, or financial crises) might be expected to have heightened the risk awareness of managers in individual port organisations. However, Beasley and Frigo (2010) observe that while the risk environment for global enterprises is expanding and becoming increasingly complex, risk managers appear to be reluctant or unmindful of the need to proactively change, adapt and add rigour to their risk management strategies to match these times and circumstances. The rationale for ports to monitor the risk environment is to gain early warning of developing or imminent hazards. Early warning provides increased potential for maintaining port business continuity, or in the event of a hazard impacting the port, to be prepared for restoring operational capabilities within tolerable downtime and acceptable cost parameters (Petterson & Schulman 2016).

This real-time risk environment monitoring and ability for early recognition of an incipient adverse event are what Weick and Sutcliffe (2015) describe as organisational 'mindfulness'. Mindful managers learn to recognise and react early to adverse events, enact proactive risk management responses and if required, adapt to dynamically changing circumstances (Parker 2010; Weick & Sutcliffe 2015). Disruption preparedness requires the prior establishment of crucial information and communications infrastructure, coupled with established information pathways for collaboration and coordination with public and private sector critical infrastructure stakeholders (Wakeman 2013; Wagner, Chhetri & Sturm 2014).

Within an Australian port context, managers' expectations of future risks against other reliable sources of risk expectations might provide an indication of port organisational risk awareness. An understanding of port 'mindfulness' to future risks would benefit from communications detailing what proactive preparations are being made to treat these expected risks, and an analysis of what preparedness gaps might exist.

4.6.7. Risk management communication and reporting

Risk management communications and reporting are complex tasks. Crucial functions include transmission of strategies, policies and plans to employees to ensure consistency in risk management approaches, evolving a sound and effective risk culture, establishing a common risk vocabulary, developing lines of coordination and collaboration within and without the port, and the services, hardware and systems that enable the communications and reporting capabilities (ISO31000:2009; ISO31010:2009; Haraguchi, Lall & Watanabe 2016; Hopkins 2017). Board responsibilities include ensuring that processes are in place for all employees to understand their risk management roles, responsibilities and accountabilities (ISO 31000:2018). Additionally, senior executives have compliance responsibilities for reporting to legal, regulatory and governance agencies both during and following a port disruption.

Port risk management communications involve the transmission of information to all employees, external stakeholders and regulatory authorities including local

emergency response agencies (Hopkin 2017). Without effective internal risk management communications, organisational risk management practices are liable to develop in a fragmented fashion (silo management) with managers from different departments planning for and managing differing types of risk with varying levels of priority, plus minimal levels of collaboration, communication and coordination (Lam 2014; Hopkin 2017). Organisational and functional silos can result in unnecessary organisational complexity and inflexibility, duplication of effort, lack of visibility, poor integration and wasted resources, with potential to hamper risk management effectiveness (Harner 2010; Fraser & Simkins 2010).

Should the port experience an unexpected and rapidly impacting disruption, then risk management performance is likely to be adversely affected by time pressures and uncertainty. Deficiencies in communication services, and unclear lines of communication within and external to the port are likely to impede decision making and collaborative responses (Houghton *et al.* 2006). Cross-agency communications and collaboration capabilities within public and private sector networks are essential to enabling crucial information flows where best needed during a disruption (Smythe 2013; Crowther 2014; Kolomiyets 2017). The port's external risk management communications and reporting channels encompass multiple networked actors with disparate self-interests and conflicting attitudes and establishing network communications is an important component in establishing network sustainability (Bichou & Gray 2005; Cahoon, Pateman & Chen 2013).

Establishing relevant regional communication networks begins with identifying critical infrastructure and emergency response agencies and framing relationship parameters - for example governance measures, rights and responsibilities, and confidentiality agreements (Carr 2016; Hunt & Greaves 2017; Kolomiyets 2017). Port risk management communications and reporting relies upon the continued availability of internet and intranet services, electrical power, telecommunications, navigational AIS systems, and VHF and UHF radio systems (Burns 2015). These systems and services are essential in exercising coordination, command and control activities in managing risk, in addition to recording key

aspects of response actions (Lansdale 2012). The port's ICT system is crucial to risk management support. Recording, monitoring and reporting processes are performed either within a generic information system, within a standalone software system, or a web or Cloud-based component of the port's integrated information management system (Kolomiyets 2017). Managers require access to risk management records to fulfil their roles and accountabilities and to share knowledge, a process supported by the port's generic information system (Chapman 2011). A risk information and document management system, according to Kolomiyets (2017) progressively enables risk management recording, monitoring, assessment, learning and dissemination of knowledge. Also, an effective risk information and document system contributes to the compilation and updating of port contingency plans.

4.7. Business continuity and disruption response and recovery

A capable port risk management framework requires avoidance of silo-based approaches to risk management, and instead the port should ensure that its business continuity management becomes closely linked with effective risk management and resilience processes and activities (Sheffi 2005; Banasiewicz 2015; Graham & Kaye 2015; Sahebjamnia, Torabi & Mansouri 2017). The port objective in developing business continuity capabilities is to lessen the consequences of disruption primarily through maintaining port system interdependencies, and in establishing alternative premises, services and resources sufficient to retain or quickly recover operational capabilities (Hiles 2011; Pettit & Lewis 2017). Business continuity as a short-term recovery measure, and disruption response and recovery as a longer-term measure, constitute the primary contingency responses of many organisations (Sahebjamnia, Torabi & Mansouri 2015). Resilience emerges within this business continuity and disruption recovery context in knowing when business continuity measures should be halted, and recovery operations commence (Sahebjamnia, Torabi & Mansouri 2015).

Whereas a risk management framework provides managers with knowledge and techniques for reducing risk, business continuity planning provides capabilities for operationalising those techniques aimed towards anticipating and reducing risk

(disruption risk reduction). Port business continuity activities include identifying hazards, assessing the risks, identifying and assessing vulnerabilities, mitigating the risks and increasing organisational preparedness to meet these risks (ISO 22301:2012; UNISDR 2015). The Sendai Framework for Disaster Risk Reduction 2015–2030 (UNISDR 2015) provides guidance of relevance to port managers in managing new and emerging risks, in reducing existing risks and for strengthening resilience. Much of this guidance relates to planning and preparations towards minimising port vulnerabilities to hazards, disruption preparedness, in relation to responding, managing and recovering from emergencies, and compilation of effective emergency response plans, capabilities, training and resources (Aitsi-Selmi *et al*. 2015; Haddock, Bullock & Coppola 2017). Aitsi-Selmi *et al*. (2015, p. 164) reflect that 'it is often not the hazard that determines a disaster, but the vulnerability, exposure, and ability of the population to anticipate, respond to, and recover from its effects'. Within a port disruption management context, this concept suggests that risk and resilience management cognisance and preparedness are largely the determinants of hazard consequences and business continuity prospects.

Critical infrastructure disruption recovery is aided by the extent and effectiveness of business continuity planning preparedness, and particularly so where a high level of technology dependencies exists (St-Germain *et al.* 2014). The importance of business continuity to port managers relates to how well potential hazards and their consequences are identified, and how well a strategic and planning framework and enabling resources are developed to prepare the port to manage the impacts of a diverse range of hazards (Graham & Kaye 2015). Little is known about Australian port capabilities in these areas.

In general, business continuity planning is based upon risk identification and assessments, vulnerability analyses, and the identification of core resources and capabilities required to maintain or return operations to serviceability within an acceptable time scale (Wallace & Webber 2017). The planning also involves identification of alternative systems, services and suppliers if disruption denies port managers access to their normal range of crucial business resources (Hiles

2011). Allied with these business continuity concepts are disruption responses, emergency management and recovery planning processes (Sahebjamnia, Torabi & Mansouri 2015). These aspects of business continuity preparedness require compilation and testing of a response plan, which is known variously as an emergency plan, contingency plan, disaster recovery plan, or disruption response plan (Sadgrove 2017). A disruption response plan should be tested at regular intervals, and Sadgrove (2017) suggests that occasionally a spontaneous exercise should be held on a weekend to ensure that the plan still works in the absence of key personnel. An alternate premises emergency centre should also be fully tested to ensure that it can support critical aspects of port operations at a pre-planned minimally acceptable level of effectiveness (Graham & Kaye 2015). Business continuity planning should also establish the longest tolerable period of operational downtime and reflect a communications protocol for communicating key disruption-related information to internal and external stakeholders (Sadgrove 2017). Performance testing through drills and exercises is improved by comparison with benchmark levels of proficiency, and Sadgrove (2017) suggests the use of a risk maturity model for this purpose.

4.8. Maturity models and performance management and measurement

An early form of maturity model is described by Crosby (1980) as a quality management maturity grid that depicted progressive levels of quality management understanding and implementation of quality improvements. The concept was then applied towards information systems research, from where the maturity modelling concept has evolved and spread into wider academic and practitioner uses. Maturity modelling facilitates either self-auditing or third-party reviews, and the use of quantitative and/or qualitative analyses. A risk management maturity model (RM^3) is described by Bititci *et al.* (2015, p. 3065) as a means of identifying an organisation's degree of:

> Formality, sophistication and embeddedness of practices from ad hoc to optimising… (and to) …position current practices of an organisation against the maturity scale (i.e. from ad hoc to optimising).

Potential questions to be asked by port Board members of the CEO are 'how well prepared are we for managing risk' and 'how does our risk preparedness compare with other organisations?' Evidence-based answers to these questions require a readily understood system of measurement and comparison, which is the purpose of a risk management maturity model. Risk management performance measurement can also be conducted by subjective judgement (value-based) means, however judgements made in consequence of past experiences may not be truly indicative of what might occur with future risk events (Thekdi & Aven 2016).

Performance measurement systems are increasingly the subject of port-oriented literature (Pallis *et al*. 2011; Woo *et al*. 2012; Langenus & Dooms 2015) so that several management and measurement framework models exist. For example, the balanced scorecard (Bourne *et al*. 2003; Bititci *et al*. 2012); the Strategic Measurement Analysis and Reporting Technique (Cross & Lynch 1989; Bititci 2015); and, the Integrated Performance Measurement System Reference Model (Bititci*,* Carrie & McDevitt 1997; Bitici 2015). Performance measurement might also be assessed through meeting progress objectives, for example those contained in the risk management framework within ISO 31000:2009. The literature provides little indication of how Australian port managers assess their risk management performance, capabilities and effectiveness in comparison with other ports. Instead. a proposed descriptive risk management maturity model at Figure 4-3 summarises the discussions of this chapter and provides a basis for assessing the effectiveness of self-reported port risk management capabilities to be acquired from the empirical research. Maturity models as shown in Figure 4-3 provide a useful technique for measuring and evaluating organisational risk management methods, processes and capabilities (Tangen 2005; Bititci *et al.* 2015).

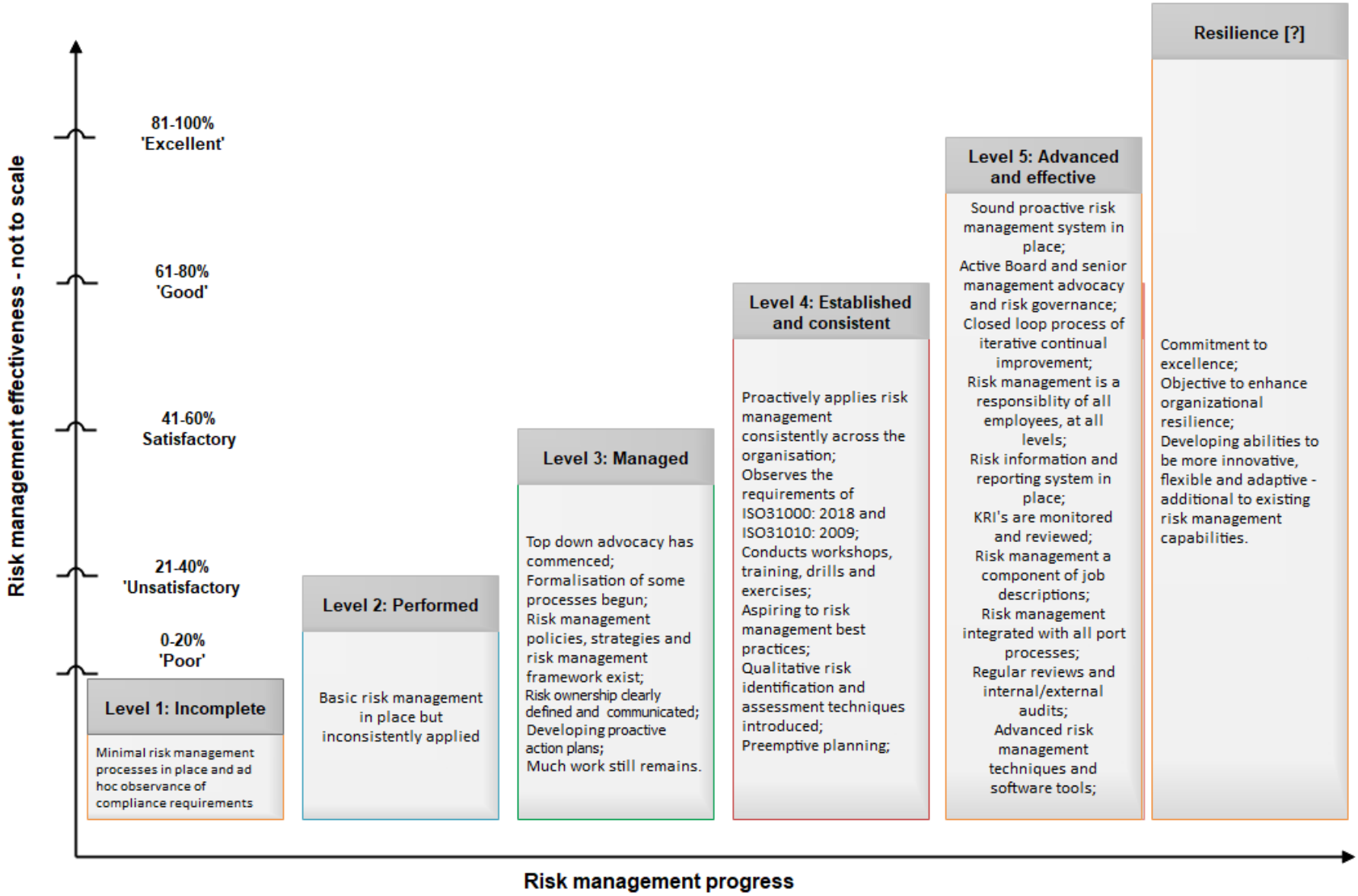


Figure 4-3: Characteristics of a port risk management maturity model (Adapted from Chapman 2011; Arrow 2012; Andrews 2017; Kolomiyets 2017).

In overview, risk management maturity models are performance measurement systems (also known as Performance Measurement and Management systems) intended to assist organisations in formulating, implementing and measuring the effectiveness of corporate objectives, strategic plans and overall performance (Wettstein & Kueng 2002; Gunasekaran & Kobu 2007; Bititci *et al.* 2012). Maturity modelling techniques also provide port managers with means to assess their progress in developing risk management capabilities, evaluate their risk management strengths and weaknesses, and assist them in formulating targets towards higher levels of capability (Chapman 2011; Jia *et al*. 2013).

4.9. Summary

Chapter 4 discussed the evolution of port risk management and reviewed risk management compliance requirements, the status of risk management frameworks and processes, and the state of research associated with port managers' abilities in managing risk. The chapter revealed that Australian port managers have access to a diverse range of guides, techniques and approaches to assist them in their vulnerability modelling, risk management capabilities, and compliance responsibilities. This chapter also revealed multiple sources of information and a risk management maturity model to assist managers in reviewing or auditing port risk management practices.

A sound risk management foundation is primarily suited to managing normative port hazards and their consequences (for example at risk management maturity level 5). These involve *known* hazards and risk probabilities. However, in managing new, emerging, unknown and unexpected port hazards with uncertain consequences, Australian port managers require additional abilities for more innovative, flexible and adaptive disruption responses in maintaining business continuity. Attainment of these additional enhanced abilities requires Australian ports to establish and promote organisational resilience capabilities and responses, using risk management and continuity processes and procedures as foundational means to this end. The degree of inability to cope using conventional risk management tools and techniques is dependent upon the degree of knowledge and certainty held by port managers – as the port risk environemnt

becomes increasingly influenced by uncertainty and new, previously unknown risks evolve, then risk management coping abilities and effectiveness declines, as shown in figure 4-4. Coping refers to port management abilities, approaches and systems to effectively understand, identify, anticipate, control and manage expected and unexpected risks and uncertainty (Van der Vegt *et al*. 2015; John et al. 2016; Renn 2017).

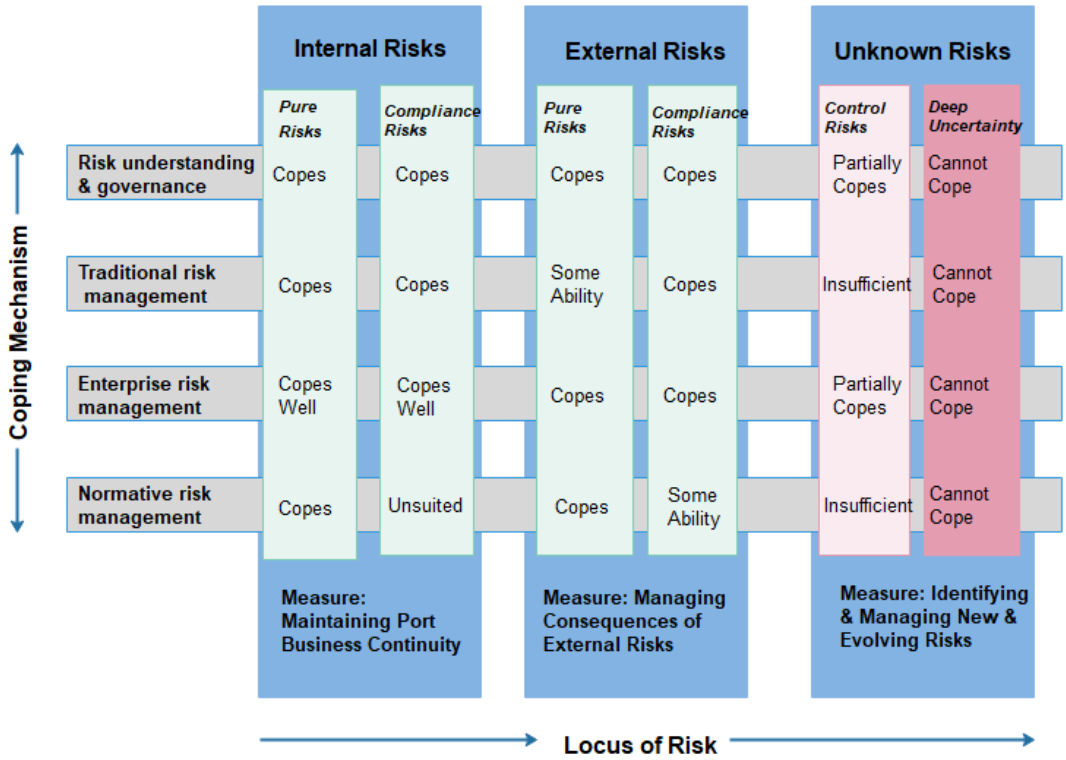


Figure 4-4: Port risk management effectiveness model to summarise Chapter 4 (Author).

Accordingly, Chapter 5 now searches the literature for what is known about resilience and assesses how it might be employed in enhancing Australian port preparedness and performance against complex and unforeseen disruptions. Chapter 5 aims to determine what drivers, resources and governance attributes might be required to operationalise organisational resilience into more effective risk management practices.

Chapter 5 - Operationalising port resilience

5.1. Introduction

Preceding chapters investigated how risk management might be employed in optimising business continuity across the port's internal and external operating environments. These chapters provided a clearer understanding of how managers strengthen and protect their port/s against the impact of known and conceivable risks within a stable risk environment (Blades 2017). Findings from these chapters demonstrate how port risk management capabilities and capacities are increasingly challenged by the potential for new, unforeseen and unpredictable global risks (WEF 2018). These uncertainties bring port risk managers to a type of stasis, where conventional risk management processes alone appear to be inadequate for treating an increasingly uncertain and unpredictable risk environment.

McManus *et al.* (2007) advocate the employment of resilience management as an alternative investment towards organisational performance and the well-being of its community of stakeholders. Similarly, the Australian Government (AG 2016) encourages critical infrastructure operators, including port managers, to build their levels of resilience as a critical supplementary capability for conventional risk management. This evolutionary improvement process reflects a global organisational and academic interest in resilience within diverse applications, for example disaster preparedness and contingency management, complex systems, and resilience management (Carralli *et al.* 2010; Cavallo 2014; Weick & Sutcliffe 2015; Adini *et al*. 2017; Doerfel & Prezelj 2017; Kim & Park 2018).

Chapter 5 investigates the state of organisational resilience knowledge and examines a notional performance measurement and management model for operationalising, managing and measuring the indicators of port operational resilience. Operationalising resilience towards managing the port's internal uncertainties and unpredictabilities (Bach *et al*. 2013) is only part protection for port operations. Port managers need to assess their vulnerabilities to failure

of the port's external critical infrastructure partners, each with their own set of internal failure modes and hazards (Carralli 2006; Hughes & Healy 2014). Chapter 5 begins by examining why port managers should adopt a heightened resilience focus.

5.2. An overview of resilience, and resilience capabilities

Resilience theory researchers appear unable to decide whether resilience is either 'a measure, a feature, a philosophy or a capability… (or whether resilience is) a tangible or an intangible capability' (Bhamra, Dani & Burnard 2011, p. 5389). This level of ambiguity lends importance to further research that aims to provide a clearer understanding of organisational resilience, and how organisational resilience might be employed to manage the uncertainties and ambiguities of the global risk environment.

Unexpected and unforeseen adverse events arising from this risk environment are sometimes referred to as 'wicked problems' or 'Black Swan' events due to the increasingly unpredictable nature of the risk environment, and the levels of complexity, uncertainty and ambiguity that arise when a wicked problem emerges (Conklin 2006; Smithson 2010; Paté-Cornell 2012; Flage & Aven 2015; Gharehgozli *et al.* 2017). Whereas existing risk management capabilities and capacities remain effective in treating known and foreseeable risks, these probabilistic approaches must be complemented by resilience capabilities to address unknown, unanticipated, and otherwise unmanageable new and emerging risks (Linkov *et al.* 2014; WEF 2018).

Multiple resilience strategies and management systems exist as a start point for organisations wanting to enhance their levels of resilience. For example, ISO 22316:2017 Security and resilience - Organizational resilience - Principles and attributes, offers a definition (2017, p. v):

> Organizational resilience is the ability of an organization to absorb and adapt in a changing environment to enable it to deliver its objectives and to survive and prosper.

Despite attempts to formalise resilience in standards (ISO 22316:2017; BS 65000: 2014) and the rise of multiple organisational resilience indicators (Seville 2008; Blades 2017) there remains a conceptual problem in quantifying organisational resilience, and in establishing how managers might achieve requisite resilience capabilities. Resilience is not a stable organisational or management attribute, rather, Chandler (2014) describes resilience as a dynamic form or style of interactive adaptation to changing circumstances. Within this context, a dynamic risk management response to an emergent hazard evolves as a complex adaptive process, in which managers proactively respond, adapt and reshape their organisational disruption management inputs (Chandler 2014).

Whereas known and stable risk conditions permit risk management more by conventional means and response by rote, complexity and uncertainty requires risk governance more attuned to resilience thinking, problem solving and self-organising, with expertise based on knowledge and experience (Walker & Salt 2012; Chandler 2014). Caralli *et al*. (2010) argue that low-resilience organisations should rethink their customary risk management processes and implement organisational resilience against unexpected high consequences risk. A management organisational resilience focus requires a clear understanding of what is important to maintaining identity and continuity of operations, an acceptance of change, empowerment of managers for flexible and considered decision-making, and organisational ability for ongoing adaption to changing circumstances (Walker & Salt 2012). Academic resources might enable managers to think within a resilience context, but only a manager deeply immersed in managing a disruption can decide what needs to be done in exercising resilience for each disruptive circumstance (Chandler 2014).

5.2.1. Organisational resilience

Resilience concepts evolved from ecology theory (Holling 1973) and are increasingly employed within natural and social science research, for example to address climate change and disaster management (Davidson *et al*. 2016). Broad platforms of resilience are *engineering resilience* in which a structure or

system is designed to operate and remain within predetermined parameters, and *socio-ecological resilience* in which a system normally operates within a set of parameters but if disturbed sufficiently to overcome its inherent resilience (Figure 5-1), it will be displaced from this state and into another (Holling 2001; Holling & Gundersen 2002). Engineering resilience is measured within the context of how rapidly a system or organisation can return from disruption to its previous state of equilibrium (Tilman & Downing 1994; Hollnagel 2014) and is characterised by efficiency, consistency and predictability (Briske, Illius & Anderies 2017). Socio-ecological resilience is alternatively characterised by persistence, change and unpredictability from a non-equilibrium theory perspective (Briske, Illius & Anderies 2017).

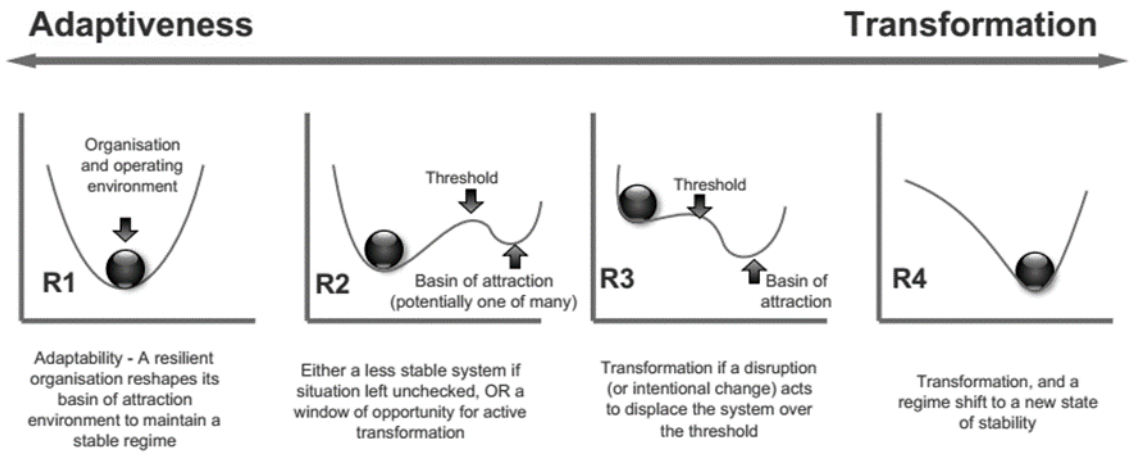


Figure 5-1: Resilience states R1-R4 showing states of transformation (Adapted from Gunderson, 2000 and, Walker & Salt, 2006).

McManus *et al.* (2008, p. 81) argue that organisational resilience might be manifested in both day-to-day operations and during emergency response and recovery, and that enablement of resilience requires '…situation awareness, management of keystone vulnerabilities, and adaptive capacity.' The model at Figure 5-1 employs a ball and basin analogy (Gunderson 2000) which is modified by the researcher to capture this continuum relationship between an organisation's awareness, adaptiveness, transformation and resilience performance.

A ball and basin analogy for organisational states has long been used to advance both scientific and management theory (Briske *et al.* 2006; Brand

2009). The level of organisational resilience is overcome when the scale of disruption is sufficient to displace the organisation (shown as a ball) over its stability threshold, and into another basin of stability (Gunderson 2000; Walker & Salt 2006). Specifically, resilience phase R1 in the model portrays an adaptive organisation, able to maintain its resilience and the stability within assigned operational parameters. At phase R2 the organisation has become less resilient and therefore more vulnerable to disruptive forces affecting its stability. At this phase of untenable operational circumstances, a mindful and resilient organisation might innovate to actively control its transformation to a fundamentally new state of business continuity stability (Walker & Salt 2006). Otherwise, sufficient disturbance will displace the organisation across the R2 transformation threshold into a new basin of attraction (R3), and, should the organisation be still unable to effectively manage the disruption, then upon eventual recovery the organisation undergoes a regime shift to a new reality (R4).

From a social science perspective resilience is an unobservable construct; it cannot be physically measured, rather its presence is inferred from outcomes to adverse events that demonstrate organisational or individual positive ability to absorb or adapt to negatively altered circumstances (Cosco *et al.* 2016; ISO 22316:2017). The international standard ISO 22316:2017 discusses 'enhancing' resilience which infers that resilience is always present even if unobservable in its varying weaker or stronger forms. Cosco *et al*. (2016) describe this varying flux of resilience as movement along a resilience continuum, rather than an abstract reactive or proactive quality that either is or isn't.

Despite an emerging concept that resilience can be beneficially applied to day-to-day problem solving (Alesi 2008; Brown, Seville & Vargo 2017), resilience researchers regard resilience as something that might not always be present and investigate how to 'embed' resilience into the topic of their research: for example, Inglis *et al.* (2014) – adapting to climate change; Bond *et al.* (2015) – environmental impact assessments; O'Connell *et al*. (2016) – sustainable development. The Oxford Dictionary of English (2010) regards the word

'embed' as meaning to implant an idea or feeling within a specific context so that this idea becomes ingrained. When Bond *et al.* (2015) discuss the concept of embedding resilience into environmental impact assessments, they propose to translate theoretical resilience deliberations into practice to overcome the adverse effects of ambiguity, uncertainty and ignorance in scientific decision making. In this sense, embedding resilience into an organisation or its practices is analogous to operationalisation, which is described within the social sciences as reconceptualising an abstract concept so that it assumes sufficient tangible meaning to be translated into more directly observable and measurable practice (Jupp 2006). An objective of this thesis is to explore how resilience theory might be operationalised at Australian ports, but first, resilience is explored for how it is perceived within wider contexts.

5.2.2. Resilience from large scale studies

Few studies explore residence within an Australian context, and to the best of the researcher's knowledge, Australian port resilience is a new field of organisational management research. An example of organisational resilience research is provided by a UK business intelligence research organisation linked to The Economist newspaper. The Economist Intelligence Unit (EIU 2015) international survey questioned 411 senior executives from primarily medium size enterprises, asking for their opinions on the relevance of resilience to their enterprises. This is a large sample number focused on a question of relevance to this thesis, and therefore of interest. Whereas 88% of these executives agreed that resilience is a priority in management considerations, only 29% of the 411 enterprises had resilience embedded within their systems and 44% had intentions to progress with enhancing their levels of resilience. Responses are shown in Figure 5-2.

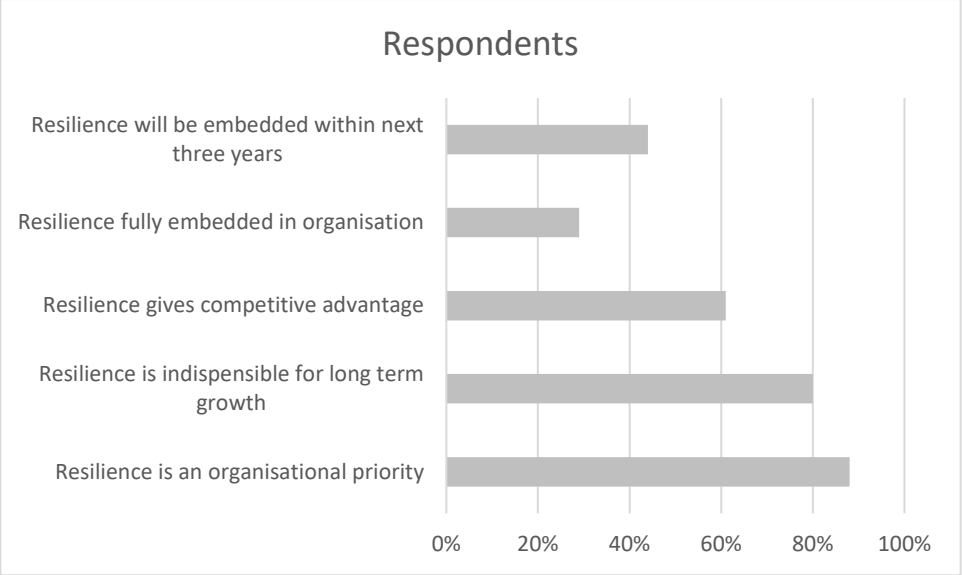


Figure 5-2: Resilience governance attributes of 411 international enterprises (Adapted from EIU 2015).

A core principal of ISO 22316:2017 that is aligned with operationalising resilience is the requirement to gain enterprise-wide commitment to, and understanding of the resilience processes, however of the 411 respondents to the EIU (2015) survey, 275 reported that resilience is inconsistently applied across their organisations. The survey covered an aspect of importance to this thesis, namely, what factors are most important in embedding resilience into an organisation. Six of the factors addressed by the EIU question appeared to be of relevance to port organisations:

a) understanding customer needs;
b) providing staff training and increasing skill levels;
c) providing effective leadership;
d) effective corporate governance;
e) information security needs; and
f) operational processes related to environmental issues.

The survey responses to these question components were assessed to gauge their suitability for use in the empirical research of this thesis. SPSS software was used for this assessment, and factor analysis reveals that for the EIU (2015) survey respondents, the influence of customer requirements most strongly influenced the implementation of organisation resilience capabilities within the

organisations. The three other factors that most strongly influenced organisations to enhance their resilience effectiveness were:

a) providing staff training and increasing skill levels;
b) providing effective leadership; and
c) effective corporate governance.

These four factors are utilised within the investigation of resilience factors within this thesis. Interestingly, 13% of the 411 international EIU survey respondents professed that the reason why they were influenced to embed resilience within their risk management processes was because resilience is 'a necessary evil – driven by regulation / a "must do it" (EIU 2015, p. 6). The EIU survey was further relevant to the research problem of this thesis, in listing respondents' opinions on what constitute the most likely sources of risk to arise over the next three years. Market competition and macro-economic uncertainty were the greatest perceived concerns.

5.2.3. Resilience within a critical infrastructure context

The Australian Government approach to encouraging critical infrastructure resilience involves establishing focused web sites, the formation of public/private partnerships, and formulating plans and strategies to guide and promote resilience principles for the critical infrastructure sectors (AG 2010, 2015, 2016, 2017; IA 2016; TISN 2016). The *Australian Government Resilience Strategy* (AG 2010) was followed by the implementation plan - *Australian Government Resilience Strategy: Plan* (AG 2015, p. 1) whose core policy objectives encourage:

> Critical infrastructure owners and operators to be effective in managing reasonably foreseeable risks to the continuity of their operations, through a mature, risk-based approach. The second objective is for critical infrastructure owners and operators to be effective in managing unforeseen risks to the continuity of their operations through an organisational resilience approach.

Specifically, the Australian government (2008) argues that senior critical infrastructure managers should insert resilience into their governance systems

by aligning resilience governance concepts with enterprise risk management, business continuity and strategic planning processes. The Australian government resilience strategy envisaged a Trusted Information Sharing Network working group, whose members include representatives from academia, business, peak bodies and government (TISN 2016). A TISN sub-group provides guidance and resources to assist the owners and operators of critical infrastructure in their resilience governance approaches.

Australian and US governments encourage critical infrastructure resilience to become a shared responsibility between the public and private sectors, whereby governments act to coordinate and promote the development of operator level resilience (Dunn, Cavelty & Suter 2009; Trucco & Petrenj 2017). Australian national and State governments encourage critical infrastructure public and private organisations (including port authorities) to enhance their resilience levels in recognition that traditional corporate strategies might not protect their entities from unexpected and unforeseen events (AG 2013). The Australian government, for example, regards an organisation's resilience as its ability for adaptation and evolution to unexpected changing circumstances and unforeseen sudden shocks, coupled with organisational capabilities for change in meeting longer term challenges (AG 2016). Factors contributing to organisational resilience are summarised within the next section.

5.2.4. An overview of resilience concepts

This section provides an overview of the major components of organisational resilience, and an indication of how the context in which resilience is viewed might influence academic and practitioner perspectives of the concept. According to Linnenlueke (2017), and depending upon the context in which resilience is viewed, resilience can be perceived as:

a) a way of rectifying internal deficiencies or shortfalls (internal audit context);
b) methods for mitigating against risks, and reconfiguring redundancy and agility processes (risk avoidance context);
c) a process of learning and bouncing back/forward (recovery context); or

d) a method for evaluating the post-disruption state (outcomes context).

Two primary contexts are engineering resilience – maintaining the organisation in an efficient stable state (Cretney 2014; Hollnagel 2014) and ecological resilience - organisational ability to absorb disruption until changing variables and processes necessitate a shift in system state (Cretney 2014; Briske, Illius & Anderies 2017). The context setting is also important in conceptualising resilience from either an internal or an external perspective, or holistically from both perspectives as when clearly and fully understanding the organisation and its key dependencies and requirements (ISO 31000:2018). Resilience is also a multi-layered concept (Obrist, Pfeiffer & Henley 2010) and so conceptualisation may be performed at strategical, operational, or theoretical levels, and, within the context of technical, organisational, social, and economic dimensions of resilience (Bruneau *et al.* 2003).

ISO 22316:2017 emphasises that there is no 'gold standard' for conceptualising resilience, only that an organisation can be regarded as more or less resilient overall. Additionally, the organisation might be more resilient in some areas and less resilient in others. An organisation's abilities to absorb, adapt and change in responding to disruption according to Kaim, Rana and Rizvi (2012, p. 23) requires modifications to '…objectives, policies, and standard routines (to challenge) …deep-rooted assumptions and norms (while taking opportunity of) …radically different solutions to problems and dramatic jumps in improvement'.

Resilience is a coping mechanism, a higher form of risk management (Dahlstrom *et al.* 2009) based on training and learning process from which managers gain ability to recognise and react early to adverse unexpected and unforeseen disruptions, enact proactive risk management responses and if required, quickly adapt to dynamically changing circumstances (Parker 2010; McCrae 2014; Weick & Sutcliffe 2015; Woods 2017). A worst-case scenario from a low resilience perspective, is that managers cannot cope with rapidly changing adverse circumstances and their organisational operations are halted (Dakos *et al.* 2015). 'Coping' literature follows a similar conceptual path to that

of resilience, with both describing attributes and strategies employed against adverse circumstances to deliver outcomes in line with objectives (Harland *et al*. 2005). At times the two lines of study converge, so that resilience is defined by Greene and Conrad (2002, p. 37) as: '…the capability of individuals to cope successfully in the face of significant change, adversity, or risk'. The consideration of resilience as an individual manager coping mechanism is evocative of the psychological approach within positive organisational behaviour theory (POB) involving '…positive traits, states, and behaviors of employees in organisations' (Bakker & Schaufeli 2008, p. 148). The empowerment of POB and autonomy within an organisation, senior management support, and encouragement towards an innovation culture (Bakker & Schaufeli 2008) are key resilience factors promoted within the Australian government resilience strategy (AG 2011). According to Gibson and Tarrant (2010) resilience evolves from sound and effective risk management and business continuity practices. An evolutionary pathway for developing port organisational resilience is proposed and justified later within this chapter.

Resilience requires high level emergency management and business continuity behaviour in responding to and recovering from disruptions. Emergency management responses alone are unlikely to provide sufficient response to manage the disruptive impacts of a crisis. An organisational emergency is likely to affect only a section or component of the organisation or its operations, whereas a crisis affects the whole of the organisation and the disruptive consequences might potentially lead to a restructuring of the entire organisational functions (Judek & Edjossan-Sossou 2017).

During normal business operations, management resilience behaviour might be tested during drills, exercises and simulation however these training methods can only prepare managers part of the way for coping with real-life crisis situations. Industry managers might learn more of resilience from the aviation industry, for example the crew crisis management conducted onboard United Airlines Flight 232 in 1989. The aircraft suffered a catastrophic engine malfunction at the tail, which ruptured hydraulic control lines following which

all conventional flight operations became impossible (Dekker *et al*. 2016). The flight crew had only the power of the two remaining engines which they employed in innovative ways by 'thinking outside the box', 'taking a system way beyond what it was designed to do', and 'making use of an adverse design quality such as pitching moments with power changes' (Dekker *et al*. 2016, p. 307). While noting that 42 simulator attempts to replicate the United Airlines 232 landing were unsuccessful, Dekker *et al*. (2016) endorse the use of simulation training for its ability to take managers beyond their comfort zones, causing them to modify their normal responses and behaviour, learning to be more adaptive and flexible in unexpected and unusual circumstances, and to be more capable of resilience behaviour during disruptive circumstances.

5.3. Organisational resilience and dynamic capabilities theory

Resilience and its opposite state of vulnerability are difficult states to measure because both are theoretical concepts (Hinkel 2011; Schipper & Langston 2015). Conceptually, resilience is an intangible organisational asset (Hall 1992) that has the capability to positively influence the outcomes of risk management, whereas vulnerability is an intangible liability that exposes the organisation to future hazards. As a theoretical concept, resilience is an intangible resource and a latent capability that becomes manifested when organisations respond to adverse challenges and rapid change (Hall 1993). Resilience responses might occur with events affecting either a component of the organisation's practices or the whole organisation (McManus *et al.* 2008). With relevance to this thesis, Hall (1993) categorises an organisation's intangible resources as functional and cultural capabilities. Functional competencies arise from staff knowledge, skills and experience, whereas cultural capabilities are manifested by the whole organisation in response to adverse challenges and change.

An organisation's internal resources and capabilities are closely linked with its long term strategic direction and performance effectiveness (Grant 2016). If conditions change to alter the organisation's strategic direction, and particularly if these changes are detrimental to organisational performance,

then managerial cognition and ability to reposition internal resources and capabilities become crucial factors in contending with strategic change and organisational transformation (Helfat & Peteraf 2015). 'Managerial cognition refers to managerial beliefs and mental models that serve as a basis for decision making' (Adner & Helfat 2003, p. 1021). Abilities to demonstrate organisational flexibility and resilience in maintaining business continuity contribute to this managerial cognitive capability (Lengnick-Hall, Beck & Lengnick-Hall 2011; Helfat & Peteraf 2015; Teece 2018). Resilience provides an organisation with competitive advantage when challenged by turbulent change, and in this respect resilience forms part of the micro-foundations of dynamic capabilities that assist in strategic change and organisational reconfiguration (Adner & Helfat 2003; Sheffi 2007, 2017). Organisational micro-foundations comprise the constituent elements and interactions that facilitate individual managers' roles in building and maintaining organisational capabilities (Barney & Felin 2013; Helfat & Peteraf 2015).

Whereas the literature provides some answers as to what organisational resilience and its values to the organisation might be, there is less evidence from a business model perspective of how an organisation might operationalise resilience at the required level, what motivates it to do so, how existing resources and capabilities are realigned, and what new capabilities are needed. To narrow this evidence gap, the researcher explored organisational theories for a suitable model to explain how managerial risk management cognition and abilities might transform towards a functional and cultural resilience capabilities mindset. Essentially, the researcher sought to establish a theoretical lens to learn how an organisation might employ resilience to move towards best organisational practice, and when challenged by adversity and rapid change, how the organisation might build competitive advantage through reconfigured capabilities and competencies. This type of problem resonates with the Dynamic Capabilities concepts of value creation and capture (Teece 2017). Multiple theoretical models might be chosen, for example operational capabilities theory and systems theory.

The literature suggests that a strong conceptual thread provides connections between dynamic capabilities theory, operational capabilities theory, and socio-ecological systems theory in formulating organisational strategy and competencies, particularly in the context of rapid and often turbulent organisational change (Teece 2018). Dynamic capabilities theory represents an organisational ability 'to integrate, build, and reconfigure internal and external competences to address rapidly changing environments' (Teece, Pisano, & Shuen 1997, p. 516). Systems theory provides a framework to enable a holistic perspective of the organisation and its dependencies, and the multiple internal and external components that contribute to resilience competencies (Teece 2018). A third connective link is provided by operational capability theory, which according to Wu, Melnyk and Flynn (2010, p. 725) involves organisation-specific capabilities that are generated by: 'sets of skills, processes and routines developed within the management system, that are regularly used in solving its problems through configuring its operational resources.' This thesis proposes the use of a dynamic capabilities model as a theoretical lens for explaining some key challenges in operationalising resilience within critical infrastructure organisations, and specifically, Australian ports. A further aim is to provide a pragmatic and more understandable management-oriented perspective of how organisational resilience processes are facilitated.

5.3.1. Organisational resilience in a dynamic capabilities context

Teece (2018) argues that both dynamic capabilities and systems theories contribute to a holistic understanding of how organisations might effectively respond to challenges and change in their operational environment. Dynamic capabilities theory particularly lends itself to studies involving middle management's bottom-up innovation in transforming new knowledge or methodology into regular use (Teece 2018). In parallel, operational capabilities theory also relates to operational innovation, in arguing that large scale transformational changes require the organisational acquisition and implementation of new knowledge, skills, practices and routines (Wu, Melnyk & Flynn 2010). Dynamic capabilities theory (Teece, Pisano & Shuen 1997) has

much in common with resilience concepts (for example, flexibility, complexity, innovation, adaptiveness, improvisation, transformation, learning, coping with threats and sudden change, managing uncertainty, systemic change, situational awareness, dynamic processes, governance and leadership (Teece, Pisano & Shuen 1997; Teece 2007; Teece 2017; Teece 2018). An explanatory Dynamic Capabilities perspective of organisational resilience, and potential areas for research are shown by a proposed model in Figure 5-3.

For organisations that become challenged by fast-changing environments, Teece (2018, p. 4) argues that managers 'need to develop organizational flexibility and resilience, which is very much in line with the dynamic capabilities view'. From a resilience purist perspective, flexibility is an element of resilience capabilities and abilities (Bhamra, Dani & Burnard 2011; Lengnick-Hall, Beck & Lengnick-Hall 2011). The application of Dynamic Capabilities theory to the operalisation of organisational resilience within the model proposed at Figure 5-2 encompasses the successive dynamic processes that challenge senior managers. Managers must initially identify the dynamic capability catalysts that precipitate organisational shift towards an enhanced resilience state. This enables the managers to devise and instigate transformational processes to operationalise resilience towards this enhanced resilience state.

Enabling procedures such as these encompass the development of operational skills, processes and routines for coping with unexpected change, uncertain and volatile conditions, rapid technological change, contingencies, crises, and socio-political events (Wu, Melnyk & Flynn 2010; Wilden & Gudergan 2015). Empirical research is needed to gain an increased understanding of what catalysts might prompt organisations to engage in this transformational resilience change, what organisational strategies can be employed in transforming and enhancing resilience capabilities, and the identification of challenges and issues around what Teece (2018) describes as 'seizing' resilience.

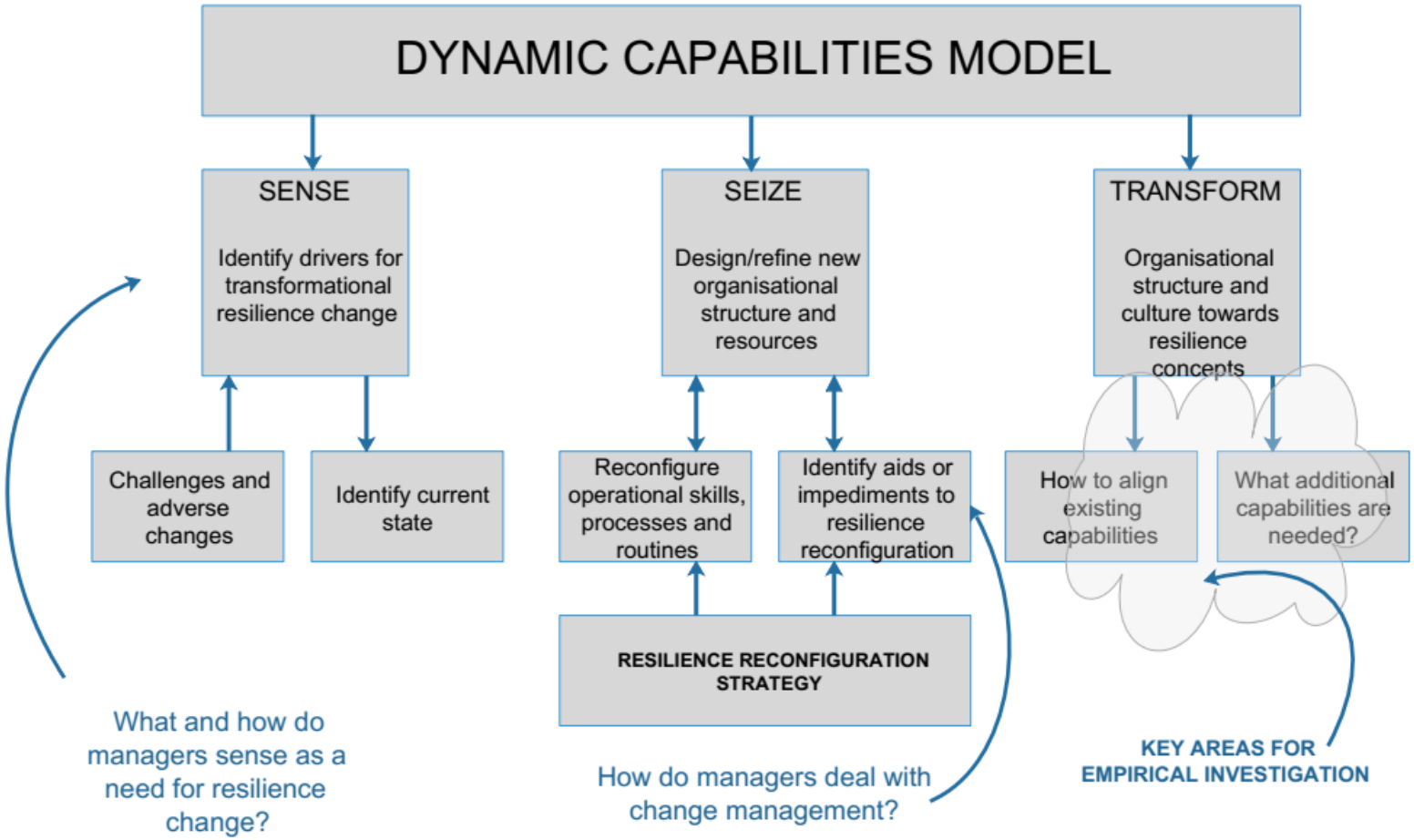


Figure 5-2: Dynamic capabilities model for transforming and reconfiguring organisational resilience (Adapted from Teece 2017).

To the best of the researcher's knowledge, dynamic capabilities theory is rarely used to identify how organisations might transform their existing operational structure and resources in response to adverse challenges and change, by employing resilience concepts to enable operational transformation and reconfiguration. Nair *et al.* (2014) propose the use of a dynamic capability framework to examine how enterprise risk management expertise is critical to effective organisational performance and survival within a turbulent environment. Ponomarov (2012) employs dynamic capabilities concepts in identifying and defining what constitutes supply chain resilience. Manfield (2016) examines from a dynamic capabilities perspective what provides the conceptual foundations for a resilience-based approach to organisations managing prolonged periods of disruptions. Kurtz and Varvakis (2016) explore the similarities and complementarities between dynamic capabilities theory and resilience theory and recommend that the theories should be integrated in small to medium enterprise strategies to better manage the consequences of disruptions. Bhamra (2018) proposes a PHD research project at Loughborough University in the UK to examine how the strategic aspects of dynamic capabilities might increase the resilience of manufacturing organisations and their supply networks. Except for the Nair *et al*. (2014) risk management contribution, these other research works examine the intersection of dynamic capabilities and resilience concepts, but only in the contexts of reviewing complementary aspects of dynamic capabilities theory and resilience theory, and what potential synergies might result from integrating the two concepts. Researchers are yet to explore through a dynamic capabilities theoretical lens how an organisation's intangible resilience capabilities, competencies and microfoundations prepare the organisation to more effectively manage the dynamic risk environment.

An investigation of transformational resilience change requires a measurement methodology that assigns numerical values to (Bahadur, Wilkinson & Tanner 2015). Organisational core capabilities in a resilience context are regarded as managerial systems, technical systems, skills and knowledge, and the governance of organisational behaviour and objectives (Leonard-Barton 1998). While the

intangibility of resilience makes transformational processes difficult to examine, indicators might provide this capability by proxy, through detecting representative activities (Levine 2014; Schipper & Langston 2015).

5.4. Organisational resilience indicators

Resilience indicators are quantitative or qualitative metrics used in identifying what is needed to build, enhance or maintain organisational resilience, and might take the form of resilience indicators, indices or scorecards (Doorn 2015; Cutter 2016). Despite the existence of multiple resilience indicator systems, there appears to be no academic convergence on what constitutes a resilience framework, by which organisations can ascertain their progress towards being resilient, or to provide warning of slippage in maintaining a resilient state (Béné 2013; Constas & Barrett 2013; Winderl 2014; Schipper & Langston 2015). An objective of this literature review is to build a port-centric resilience maturity model by using organisational resilience framework measurement principles and indicators from within the literature. Key areas of measurement under consideration for this process include system management, complexity, and the relationships that exist between resilience and vulnerability concepts (Constas, Frankenberger & Hoddinott 2014).

Indicators are integral components in the design of a resilience framework (Schipper & Langston 2015). Within a resilience framework, indicators provide dynamic, contextual and composite data for measuring progress in enhancing resilience, or slippage in resilience capabilities and effectiveness (Francis & Bekera 2014; Schipper & Langston 2015; Pitilakis *et al*. 2016). Care must be taken in drafting these indicators, because differing definitions, emphasis and operationalisation of resilience might lead to inaccurate, imprecise or skewed resilience performance measures (Doorn 2015). Further, judgement must be used to compile sufficient numbers of indicators across the range of organisational resilience attributes, because in isolation or small groupings some indicators may not appear relevant to resilience or be too small a group to enable trends or framework themes to be identified (Schipper & Langston 2015).

5.4.1. Conceptualising appropriate indicators of port resilience

A problem arises in determining appropriate indicators to identify the value of what contributes to functional and cultural attributes of resilience, particularly made difficult because there is little convergence within the literature on a precise resilience definition (Bhamra, Dani & Burnard 2011). Also, predictive indicators of resilience are likely to be subjective in nature because the effectiveness of organisational resilience is only likely to become apparent when an adverse situation or change occurs.

Researchers employ indicators consisting of 'inputs, processes, outcomes and outputs' become 'proxies' for operationalising resilience theoretical constructs into organisational practice (Levine 2014; Schipper & Langston 2015, p. 12). The types of indicator depend upon the context of the research problem and indicator purpose, for example, a set of indicators to specifically measure climate change resilience might differ in characteristics and number of indicators when compared with those to measure cyber-threat resilience (Schipper & Langston 2015). In the event of complex resilience situations with interacting and compounding risks, mathematical or software evaluations of multiple indicators might be required to assess organisational risks that cannot be measured using one indicator alone (Saisana & Cartwright 2007; Hollnagel 2017).

In the context of academic research and for practitioner relevance, organisational resilience indicators are simplified measurements of performance in optimising business continuity against high consequence hazards (Rose 2017). Specifically, Rose (2017) argues that compilation of resilience indicators should reflect:

a) all categories of major threats;
b) all resilience dimensions affecting operations management in achieving business continuity;
c) identifying factors that either facilitate or impede resilience enhancement;
d) factor weightings; and
e) evaluation of areas in which resilience might be improved.

The Rose (2017) proposals for selecting resilience indicators cannot be fully met, since not all categories of major threats will be known by management. However, the suggested approach is a logical progression from hazard identification to vulnerability assessment, preparing the most effective responses to meet the threats, and for continual improvement. These proposals are not indicators, rather, they are processes to assist in identifying and compiling resilience indicators. A further proposition for compiling resilience indicators is to adopt a top-down methodological approach (Cutter 2016), an approach suggested by the Australian Government's on-line self-administered resilience 'health check' (AG 2016). This health check employs a resilience scorecard with generic critical infrastructure resilience indicators as shown in Table 5-1. The Likert-type scorecard requires respondents' opinions on compliance within three categories of resilience - leadership and culture, networks and partnerships, and change readiness (AG 2016). Enablement factors used to assess each resilience category are listed beneath the respective sub-headings.

Indicators of organisational resilience		
Leadership & culture	**Networks & partnerships**	**Change readiness**
Strong leadership	Effective partnerships	Unity of purpose
Employee engagement	Leveraging knowledge	Proactive posture
Situational awareness	Breaking silos	Planned strategies
Decision making	Internal resources	Stress testing plans
Innovation & creativity		

Table 5-1: Indicators of organisational resilience (Adapted from AG 2016).

Table 5-1 lists 13 enablement factors across three categories of resilience management, with a total of 74 resilience indicators associated with these three categories. For example, 'internal resources' within the category of Networks and Partnerships has three indicators of effectiveness (AG 2016, p. 2):

a) IR1 - The organisation can rapidly scale up or reallocate other business resources (such as finance, premises, plant, equipment, supplies) if required;
b) IR2 - The organisation's structures, systems and processes are designed to maximise operational flexibility; and

c) IR3 – The organisation has strong liquidity and cash flow position and can absorb the impact of modifying operations to respond to challenge or adverse event.

These Australian Government resilience indicators primarily address an organisation's high-level governance, collaboration and strategic management capabilities for withstanding high consequence disruptive shocks. The health check emphasis (AG 2016) on retaining a stable operational situation (robustness) is suggestive of engineering resilience concepts, which focus on retaining an original configuration or operational status quo (Tilman & Downing 1994; Hollnagel 2014). Also, the Australian Government indicators of organisational resilience focus upon management behaviour in managing known probabilities of risk, rather than identifying indicators to measure organisational agility, adaptiveness and transformation capabilities in response to deep uncertainties (ISO 22316:2017).

Socio-ecological systems should manage the unpredictabilities and uncertainties of the contemporary risk environment less by being robust, and more by adopting adaptiveness and transformative abilities (BS 65000:2014; IS ISO22316:2017; Teece, Peteraf & Leih 2016). Of the 74 resilience scorecard indicators listed in the AG (2016) resilience health scorecard, one indicator specifically addresses the technical dimension of resilience in querying the availability of physical system premises, plant, equipment and supplies (AG 2016, IR1). One indicator, IR3, specifically addresses the economic dimension of resilience, in querying whether the organisation has strong liquidity and cash flow position and can absorb the impact of modifying operations to respond to challenge or adverse event. Otherwise, the scorecard focuses upon governance and leadership aspects of organisational resilience.

Researchers argue that four dimensions of resilience should be considered when evaluating resilience effectiveness, namely technical, organisational, economic and social dimensions (Ouyang & Dueñas-Osorio 2014; Labaka, Hernantes & Sarriegi 2016). These dimensions are discussed further within the next section. The resilience definition provided by ISO22316:2017 refers to the organisation's

capacity to absorb and adapt to the vagaries of a changing environment, which is a socio-ecological perspective of resilience (Folke 2016; Folke *et al.* 2016). The Australian Government (AG 2016) resilience indicators are not completely reflective of the adaptive and transformational aspects of socio-ecological resilience. However, the AG (2016) scorecard does provide a useful number of factors for investigation within this research and provides a list of enabling actions to overcome potential impediments and constraints against resilience.

Measuring resilience effectiveness within a major crisis context is another consideration, and due to the front-line hazardous nature of real-life situations, analysis is likely to be a retrospective task. Simulation of a successful crisis recovery situation might also be difficult to replicate. For example, as discussed separately, the flight crew of United Airlines Flight 232 in 1989 managed to fly and land a very damaged aircraft by unique means, but 42 other equally trained and experienced flight crews were subsequently unable to replicate this feat in aircraft flight simulators (Dekker *et al.* 2016). Crises management strategies and capabilities might be tested, or management training conducted, by means of crises scenario enactments or simulations (Judek & Edjossan-Sossou 2017). However, even scenarios based on real-life crisis situations might not effectively replicate the suddenness and unexpectedness of a crisis, extreme time pressures for reactions, stress and anxiety, inability to apply known responses and resources, and multiple other pressures (Judek & Edjossan-Sossou 2017). Other than enactments and simulations, organisational resilience might be estimated through the survey-based deployment of resilience indicators (Hosseini, Barker & Ramirez-Marquez 2016).

5.4.2. Employing indicators for testing organisational resilience

Cutter (2015) argues that it is not feasible to devise a comprehensive set of resilience indicators to measure all facets of resilience for all organisations, because of differing organisational objectives, differing structures and dependencies and varying categories of hazards to manage. Instead, resilience indicators must be modified to best fit the case under study. Composite indicators can be designed to test both risk management and resilience in what Cutter (2015,

p. 7) describes as risk being '…overlain by a resilience layer in order to assess the intersection of risk with resilience'. Resilience assessment tools can be designed for multiple contexts, for example top-down or bottom-up approaches, local or global settings, or focused upon operational, technical, economic and social dimensions of resilience (Ouyang & Dueñas-Osorio 2014; Cutter 2015; Labaka, Hernantes & Sarriegi 2016).

McManus *et al.* (2007) investigate organisational resilience from an operational perspective to derive a set of 15 resilience indicators. These indicators refer to resilience categories of situation awareness, management of keystone vulnerabilities, and adaptive capacity. Five indicators are developed for each resilience category. Stephenson, Vargo and Seville (2010) identify an additional eight resilience indicators and Table 5-2 provides a composite list of the McManus/Stephenson resilience indicators, shaded grey to indicate where Stephenson, Vargo and Saville (2010) added their contributions. Stephenson, Vargo and Seville (2010) and McManus *et al.* (2007) take a top-down and bottom-up approach to compiling resilience performance indicators for organisations operating within an enterprise risk management framework (ISO 31000:2018; Robinson, Francis & Hurley 2013).

Indicators of organisational resilience			
Situational awareness	**Keystone vulnerabilities**	**Adaptive capabilities**	**Resilience ethos**
Roles and responsibilities	Risk management and planning	Silo mentality management	Commitment to resilience
Hazards and consequences	Exercises	Communications and relationships	Network perspective
Connectivity awareness	Internal resources	Strategic vision	
Insurance	External resources	Information and knowledge	
Recovery priorities	Connectivity	Leadership and management	
Internal and external situation monitoring and reporting	Robust processes for identifying and analysing vulnerabilities	Innovation and Creativity	
Informed decision making	Staff engagement and Involvement	Devolved and responsive decision making	

Table 5-2: Indicators of organisational resilience (Adapted from McManus et al., 2007; Stephenson, Vargo and Seville, 2010).

Stephenson, Vargo and Seville (2010) employ components of the Table 5-2 list of resilience indicators to measure the resilience of 68 organisations within multiple industries in Auckland, New Zealand. A web-based survey with 249 respondents used a four-point Likert scale format for its questions, with responses ranging from 'strongly agree' to 'strongly disagree'. The responses were coded into percentages and averaged across each organisation where multiple managers responded to the survey. Responses were then graded within six score boundaries: 0-41% (very poor resilience), 42-50% (poor resilience), 51-59% (unsatisfactory resilience), 60-78% (satisfactory resilience), 79-87% (good resilience), and 88-100% (excellent resilience).

Most respondent organisations scored between 60-78% across the categories of performance, which the researchers argue to be a good score, one that is indicative of organisational support and commitment to resilience, adaptiveness and situational awareness. However, 35% of the organisations scored from very poor to unsatisfactory in managing keystone vulnerabilities, and no organisation scored higher than satisfactory in vulnerability management. Keystone vulnerabilities refer to components within the organisation that, if affected by a major disruption or extended severe stress, might lead to organisational collapse (McManus *et al.* 2008). While not a conclusion of their study, Stephenson, Vargo and Seville (2010) show that the surveyed New Zealand organisations report being better equipped to manage conceptual issues (resilience ethos, situational awareness and adaptive capacity) than the practicalities of managing keystone vulnerabilities. Vulnerability identification, analysis and management should be regarded as an inseparable component of risk management (Aven 2007; ISO31000:2009; Hopkin 2017), where vulnerability reflects the organisational susceptibility to hazards, and risk is a function of vulnerability and potential hazard consequences (Khazai *et al.* 2015). The New Zealand organisational difficulties in managing vulnerabilities (Stephenson, Vargo & Seville 2010) indicate that rather than endeavouring to improve their levels of resilience, these organisations might gain shorter term and more useful benefit by improving their underlying risk management capabilities and capacities.

Following this line of risk management contextual thinking, the resilience indicators listed in Table 5-2 might also be regarded as composite risk/resilience indicators that are weighted in numbers towards resilience (Beccari 2016; Wolke 2017). The Table 5-2 indicators appear to be best suited for measuring day-to-day resilience, where managers either engage in organisational learning or devise unique and innovative solutions to complex but relatively minor problems (Lyles 2014). It is unclear whether these resilience indicators are a predictive tool for gauging likely resilient behaviour, whether the indicators are restricted in usefulness to measuring past resilient behaviour, or whether the indicators are intended to measure organisational functionality and culture for conditions likely to promote resilience behaviour and thinking. However, aspects of the indicator scales developed by the Australian Government (AG 2016), McManus (2007) and Stephenson (2010a) become useful in conceptualising a port resilience framework.

The Stephenson, Vargo and Seville (2010) resilience indicator measurement tool was redeployed by Brown, Seville and Vargo (2017) with minor amendments to the Likert scale (increased to an 8-point scale), modified vulnerability management of 'external resources' to 'effective partnerships', and addition of several further questions to some resilience indicators. Two hundred and nineteen critical infrastructure employee surveys were returned, including 36 from road, rail and port employees. The objective in the 2017 study, which was well analysed in detail, was to assess resilience strengths and weaknesses in selected New Zealand critical infrastructure organisations. Major findings of the study were that effective partnerships with external organisations were the strongest contributor to individual organisation resilience, and that the two highest perceived risks to respondent organisations were reputation damage and regulatory change. Lowest scoring resilience indicators involved reluctance to break down silo management practices, and reluctance to conduct emergency and business continuity exercises and drills. While the Brown, Seville and Vargo (2017) study employed generally the same resilience indicators compiled and used by Stephenson, Vargo and Seville (2010), a more detailed application and analysis of the indicators as a

benchmarking tool proved the worthiness of the indicator framework and approach. Concepts from the McManus/Stephenson measurement tool are adapted for the design of this thesis empirical research.

In summation, resilience assessments utilise indicators of resilience when evaluating organisational capacities or potential for responding to specific hazards, for example those indicators relating to coping and adapting capacities (Norris et al. 2008; Wu, Melnyk & Flynn 2010; Wilden & Gudergan 2015; Parsons & Morley 2017). An improved understanding of resilience strengths and weaknesses provides a measure of organisational resilience maturity, and a guide for where resilience capacity building might be most beneficial (Parsons & Morley 2017). Post-incident guidance towards resilience capacity building includes learning, adaptation and transformation, which for a mindful organisation (Weick & Sutcliffe 2015) provide valuable strategic feedback learning (Folke *et al.* 2016; Berkes 2017; Parsons & Morley 2017). This continual improvement feedback loop enhances organisational resilience planning, preparation, response and recovery processes which are now explored from a port perspective.

5.5. Port resilience

Previous sections provided a general understanding of resilience, and its applicability to organisations challenged by crises. Resilience is promoted by the Australian government as a way of safeguarding critical infrastructure inclusive of ports (AG 2015), and the discussion turns now to an exploration of resilience within a port context. Before 2010, the literature rarely mentions port resilience, as noted by Vilco, Ritala and Hallikis (2012) and McEvoy *et al.* (2013). This situation seemingly altered due to the emergence of port-centric climate change research (Becker *et al*. 2015; Chhetri *et al*. 2015; Yang *et al.* 2015; Cahoon *et al.* 2016; Zhang, Ng & Becker 2017; Gharehgozli *et al.* 2017). Port resilience is further researched within the literature from multiple perspectives, including natural disasters (Shafieezadeh & Burden 2014), path dependencies (Ramos 2017), risk governance and disaster reduction (Wakeman *et al*. 2017), and cyber-threats (Meyer-Larsen & Müller 2018). This thesis engages in a broad exploration of port resilience from a

holistic organisational perspective that centres upon the stability of intermodal operations.

Resilience within a port's organisational context refers to how individual managers and the collective organisation respond to intermodal operations disruption and return their port operations to a stable state. Port resilience comprises a capability to be innovative in managing small scale emergency events within components of the port's operations, plus an ability to draw upon risk management capabilities and capacities at a superior level to manage unexpected and unforeseen major disruptions. McManus *et al*. (2008) describe this dual role aspect of resilience as having organisational abilities for resilient day-to-day operations, plus a resilient response and recovery capability in reserve to deal with crises situations.

Ports must manage a risk environment where new and unforeseen risks emerge and existing risks (for example storm events) become more severe (WEF 2018). Consequently, not all port risks can be identified and assessed, and conventional business continuity plans and emergency responses may be ill-suited as risk response and management solutions (Blades 2017). Instead, port decision-makers must develop resilience abilities to provide innovative responses and adaptive measures to recover effectively and expediently (Walker & Salt 2012; Blades 2017). When resilience becomes a mature process, port risk management effectiveness is enhanced beyond what conventional risk management might achieve on its own (Vonck, Notteboom & Dooms 2017; Wei, Chen & Rose 2017).

Port resilience is conceptually founded upon the principles of organisational resilience, which, according to Davidson *et al*. (2016, p. 26) is largely patterned around systems theory measures of '…adaptability, transformability, self-organization, and learning' - all of which have their place in a resilience framework.

5.6. Port resilience framework

Resilience frameworks and indicator measurement tools were discussed in Section 5.3 and a generic framework model for risk management (ISO 31000:2018) was reviewed in Chapter 4 and modified to reflect the port risk environment. The resilience standard ISO 22316:2017 also presents a resilience framework but not

to the same degree of detail as that contained in ISO 31000:2018. A resilience framework differs from a risk management framework because a major shortfall of the enterprise risk management framework (ISO 31000:2018) is that its use is confined to known and foreseeable hazards with determinable levels of severity (Fiksel *et al.* 2015). Resilience aims to deal with unforeseeable and unexpected hazards and their consequences (Weick & Sutcliff 2015).

Port enterprise risk management takes a reductionist perspective of risks and treats each risk as an individual case (Inan, Beydoun & Opper 2016; Hopkin 2017). The risk management framework capability gap widens when risk managers overlook potentially worsened outcomes from interactions between multiple simultaneous risks, and when the port's crucial goods and services suppliers are also impacted (BS 65000:2014; Fiksel et al. 2015; Robinson & Shewitz 2017; Haimes 2018). The need for a port resilience framework 'add-on' arises to close this risk management capability gap in the following dimensions of disruption management effectiveness:

a) Technical resilience: the port's physical capabilities, resources and capacities in support of disruption management;
b) Organisational resilience: the port's ability to adapt and evolve in line with changing external influences including market dynamics, to respond to short term shocks from natural or intentional causalities, and transformational capabilities for meeting long term challenges;
c) Economic resilience: the port's capacity to recover from or manage the adverse consequences of external economic shocks, or to have financial resources sufficient to cover the costs of crisis management and recovery; and
d) Social resilience: the port-centric system's adaptive and learning capacity to self-organise and maintain system function in support of port operations in response to regional change or disruption (Lindbom *et al*. 2014; Ouyang & Dueñas-Osorio 2014; Shaw, Scully & Hart 2014; AG 2016; Labaka, Hernantes & Sarriegi 2016).

A systems-based understanding of port systemic resilience is characterised by the degree of change that the system might sustain while maintaining form and structure, its ability to self-organise, and its ability to learn from and adapt to a disruptive event (Cumming *et al*. 2005). This understanding begins by examining how port emergency management and business continuity processes contribute towards the attainment of resilience.

5.7. Links between emergency management response and resilience

Australian port emergency response is managed along the lines of the Australasian Inter-Service Incident Management System (Lansdale 2012; Worboys 2015; Hayes & Owen 2017). Owen and Hayes (2017) describe the incident management process as a layered emergency management system involving managers at strategic, tactical and operational levels. Their findings are adapted and conceptually associated with corresponding layers of resilience management behaviour as shown in Table 5-3. Within a resilience context, superior performance at each of these three levels of management appears to be what differentiates resilient performance from conventional risk management behaviour.

Senior port managers within an emergency operations centre engage in coordination and control activities to proactively manage response personnel and physical resources, and in reaching safe, timely and optimal outcomes (Worboys 2015; Hayes & Owen 2017). However, senior managers decision-making may generally occur remote from the front line of emergency management, and Owen and Hayes (2014) argue that emergency events do not necessarily play by the rules. If senior decision-makers direct response activities without full information or ability to observe rapidly changing circumstances, then elements of uncertainty and complexity might result in emergency response team members working in unsafe and unstable conditions (Hayes & Owen 2017). Under such conditions, team member abilities to improvise, adapt and innovate in providing effective responses to extreme circumstances become crucial front line operational resilience attributes.

Emergency Management Layers	Emergency Management Tasks	Resilience Behaviour	Reference
Strategic	Whole of crisis management, external communications, and organisational oversight.	Resilience governance, leadership, direction and overall control, resolution of conflicts and crisis management effectiveness.	Alpaslan, Green and Mitroff, 2009 AS/NZS ISO 31000:2018 Tarrant, 2010 Owen and Hayes, 2014 Bhandari, Owen and Trist, 2015
Tactical	Incident response, containment, coordination and provision of resources, monitoring and record keeping,	Combining the most relevant aspects of emergency management and business continuity plans and processes to contain and mitigate the situation, and cope with rapid change. Adaptive and flexible decision-making and responsibility for all incident management activities and utilisation of resources. Responsibilities for directing teams and units to carry out emergency response activities to meet incident control goals and objectives.	Bigley and Roberts, 2001 Tarrant, 2010 Lansdale, 2012 Owen and Hayes, 2014 Bhandari, Owen and Trist, 2015 Hayes and Owen, 2017
Operational	Frontline response teams, focused on specific tasks and desired outcomes	Improvisation, innovation, adaptiveness, and efficiencies in carrying out directed responses to disruptive situations.	Bhandari, Owen and Trist, 2015 Haddock, Bullock and Coppola, 2017 Hayes and Owen, 2017

Table 5-3: A conceptual organisational structure for resilient incident management (Adapted from Owen & Hayes 2017).

Port security intelligence is provided by the Attorney General's office through the Australian Government's Trusted Information Sharing Network (TISN), a security-oriented organisation formed in response to the 9/11 and Bali bombing terrorist attacks (Sheehan 2013). Critical infrastructure sectors including ports (as elements of the TISN transport sector) are assisted in their resilience understandings by an advisory group (Sheehan 2013) whose role is to:

> Provide strategic thinking on organisational resilience, and help develop guidance and advice on tools and other initiatives that will support the owners and operators of critical infrastructure to adopt an organisational resilience approach (2013, p. 15).

Port managers who are members of the Transport Sector Group participate in resilience-oriented exercises, conferences, briefings and education on matters including best practice guidance, emergency planning, disaster response and recovery, and information sharing with other sector groups (Sheehan 2013). This provides opportunities for resilience knowledge to be transferred to respective port management organisations and instilled across the layers of management.

5.7.1. Governance and leadership

Port corporate governance is a system for assigning and coordinating activities and accountabilities for regulating and overseeing enterprise-wide conduct, and the sub-element of risk governance is an important control mechanism in achieving corporate objectives (Dahms 2008; Lark 2015; du Plessis, Hargovan & Harris 2018). Port risk governance systems are unlikely to cope with every type of adverse situation, and the literature is indecisive about an optimal model of risk governance (Christensen, Lægreid & Rykkja 2016). Researchers do largely agree that important characteristics of resilience-oriented risk governance are acquired abilities to engage in collaborative learning, change management, innovation and adaptation in circumstances of deep uncertainty and complexity (Chaffin, Gosnell & Cosens 2014; Scolobig *et al.* 2015; Berkes 2017). Tension arises between port corporate governance involving risk and resilience because risk management involves consistency and predictability, whereas resilience is managed with a freer hand and outcomes are likely to be variable and unpredictable (Lebel *et al.* 2006; Ebbeson 2010).

The Australian Government encourages critical infrastructure managers to become more resilient (AG 2015), but there is little guidance for port managers to understand and manage the complexities of this process. Complexities arise when port managers modify an existing risk management system for managing business as usual and begin to 'add-on' resilience capabilities to this stable risk governance system (Duit *et al.* 2010). The successful integration of resilience into port corporate governance requires an ability to manage the inherent tension between managing stability and uncertainty (Duit *et al*. 2010; Farjoun 2010) and this process requires well-informed, committed and strong organisational leadership.

The implementation and enactment of systemic resilience behaviour by port actors requires a holistic understanding of disruptive risk causalities, and how disruptions might affect port operation capabilities (Fisher 2011, 2013). Key risk managers need to understand what indications of stress or disruption are meaningful in terms of potential tipping point vulnerabilities, and which of these indications can be discounted (Fisher 2011, 2013). Fisher further argues that capable leadership is required to coordinate individual capabilities and capacities to respond, manage, recover, and possibly adapt to an altered state of operations following disruption. However, despite the beneficial effects of good governance and sound leadership in avoiding piecemeal responses to uncertainty, if disruptive forces exceed port resilience capabilities or abilities to adapt, then port operations might ultimately fail, and the leadership emphasis then transmutes to the transformative recovery of systems and processes (Janssen, Anderies & Ostrum 2007).

With diverse challenges emerging from a dynamic risk environment, resilience change offers benefits to port managers. Van der Vegt *et al.* (2015) argue that while conventional command-and-control organisation structures might perform effectively in a stable operating environment, they are less likely to cope with an adverse and rapidly changing operational environment. Organisations with a more flexible organisation structure and a resilience-oriented culture might adapt better through:

a) decentralised decision-making capabilities;
b) deferment to expertise and interconnected teamwork in crisis management, rather than to hierarchical position holders; and
c) empowerment of innovative and adaptive behaviour in dealing with the uncertainty of 'wicked problems' (McManus *et al*. 2008; Herrick & Pratt 2012; Andersson & T*o*rnberg 2018; Tanner *et al.* 2018).

Ports may not have a commitment to resilience, and their governance culture might place impediments in the way of resilience. As discussed in Section 2.3, evidence exists that Australian port authority management styles lean towards government bureaucracy behaviour (Everett 2007) that manifests in mechanistic

management processes and cumbersome and rigid governance, operational and flexibility outcomes. Other researchers note that organisational resilience capabilities are impeded if not curtailed by formalistic tightly controlled leadership styles (McManus *et al.* 2008; Van der Vegt *et al.* 2015). Sakalayen (2017) finds evidence that some Australian regional port managers demonstrate capability shortfalls in the management areas of flexibility, governance, long term planning, leadership initiatives and innovation. Shortfalls of this nature potentially lead to the formation of a robust but brittle state of disruption preparedness, in which the port confronts disruptive shocks by persisting with fixed risk management strategies, plans and response capabilities (resistance) rather than adaptive and transformative resilience mindsets and behaviour (Welsh 2014).

5.7.2. A conceptual port resilience implementation framework

A port resilience implementation framework should present a blueprint for the application of resilience concepts into port management practices, inclusive of strategies, plans, processes and techniques to be used in attaining the required level of capabilities and capacities (ISO 22316:2017). This type of framework is focused upon operationalising resilience and while reflecting best risk management practices, should not drill down into the detailed processes by which resilience is enacted. That is the task of a second type of framework, which is a management guideline for organisational resilience responses to disruptions (Burnard & Bhamra 2011). A third type of resilience framework measures the effectiveness of organisational resilience (Hughes & Healey 2014). A conceptual port resilience implementation framework (Figure 5-3) is constructed from the preceding resilience discussion, plus concepts outlined in ISO 22316:2017.

The decision to focus upon resilience as a further means of safeguarding the port's operations needs to be justified, through resilience learnings, knowledge and subsequent analyses of the benefits that higher levels of resilience might bring to the port organisation. Subsequently, a management case is likely to be made to the Board for endorsement and top-down advocacy of organisational common observance of resilience concepts and associated port policies and directives. In a similar way to the risk management framework described at Section 4.6,

implementation of the resilience framework is performed by middle management from a bottom-up approach. The first steps require port managers to examine and record their port afresh from internal and external resilience contexts, and to analyse the levels and locations of resilience competencies within the port system (Häring *et al.* 2017).

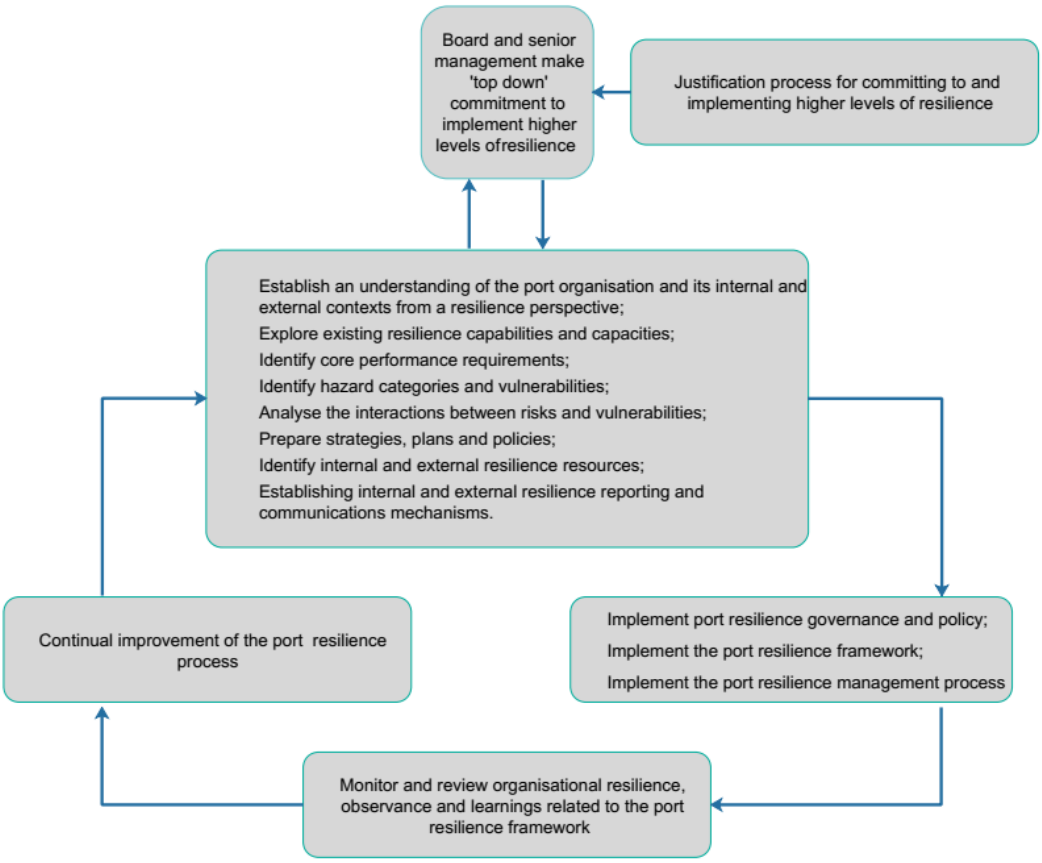


Figure 5-3: Conceptual port resilience implementation framework (Adapted from ISO 22316:2017 concepts).

Further steps in implementing higher levels of resilience (Häring *et al.* 2017) involve a review of what internal and external core system factors and enabling requirements might be integral to port operations, and what redundancies or alternatives to these system factors, properties and resources might be called upon in disruptive circumstances. As with the risk management framework (S 4.6), hazard and vulnerability identification and assessment are required. Additionally, for resilience, the port managers must attempt to conceptualise what unforeseen and unexpected disruptions might occur, and where/how the port operations might be vulnerable. This hazards and vulnerabilities process is expanded to surmise what might occur and be required in response should two or more hazards

and/or vulnerabilities combine or interact. Potential consequences of disruption must be examined to conceptualise what systems, plants and processes might fail and what the consequences of these failures might mean to operations (Häring *et al.* 2017). Administratively, the formal resilience implementation process and its associated communications, recording and reporting requirements are supported by strategies, plans and policies.

Resilience document control is rarely mentioned in the resilience literature; however, documentation appears to have an important role in the management of all critical infrastructure resilience programs and resilience documentation control could provide an interesting field of post-doctoral investigation. Documentation must be raised and managed for multiple factors of resilience (Labaka-Zubieta 2013), inclusive of the internal and external aspects of technical, organisational, financial and societal dimensions. Plans, policies and budgets must encompass all port departments and ensure that relevant crises management plans and resources are available when and where needed. Communication, collaboration and compliance with external organisations must be managed, particularly where external organisations are the nominated hazard managers for adverse events in port (AG 2011; Labaka-Zubieta 2013). The compilation of information within the documentation system should also include listings of internal and external resources that can be called upon during crisis management (Note 6). Documentation control should also incorporate the internal and external processes for resilience reporting, communications and situational monitoring. With the increasing prevalence of cyber-threats, data storage integrity becomes an important resilience management consideration.

Thereafter the conceptual resilience implementation framework follows similar closed-loop processes as the risk management framework outlined at Section 4.6. These resilience processes encompass the implementation of:

a) resilience governance and policies,
b) the wider enabling requirements of the resilience framework, and
c) port resilience management processes.

The process moves to processes of monitoring and review of all aspects of resilience practices, and learnings from resilience experiences. The final objective of the implementation framework is to establish means of continual improvement and management ongoing participation in resilience-related activities. Some aspects of this conceptual resilience framework are intended to be tested within the empirical research, however a full testing is beyond the scope of this thesis. The framework relies extensively upon port resources to fulfil resilience requirements, and this section is fleshed out with a short discussion about the type of resources that might be integral to implementing a heightened level of resilience. Much contained within this conceptual framework forms part of an extensive body of organisational resilience literature.

5.7.3. Port resources management

Resources required for building and maintaining port resilience differ from what is needed for conventional risk management (ISO 31000:2018; ISO 31010: 2009). Resilience is associated more with unpredictability, a factor affecting port managers who are unable to specify what or when new and unforeseen risks might emerge to harm their operations (WEF 2018). Wildavsky (1997) lists resources in support of resilience as the sourcing of sufficient knowledge, communications, financial and organisational capabilities and capacities to perform whatever is required, whenever it is needed.

Port managers need to justify any new expenditure in resources, cost, time and effort to their Board and accordingly, operationalisation of resilience likely requires a cost benefit analysis. In an era of extensive port reform and State budget deficits forcing State governments to draw heavily upon port revenues, some ports might be unable to justify expenditure upon building resilience. Resilience expenditure might be substantial, and the Australian government (AG 2016) identifies some expensive prerequisites for operationalising resilience. These include strong liquidity and cash flow position, premises, plant, equipment, supplies, structures, systems and processes, operational flexibility capabilities and competencies sufficient for managing the impact of adverse events. However, some of these resources coincide with those required in the conduct of enterprise

risk management (Belluz, Fraser & Simkins 2014) and may already exist in port management practices and stores inventories. Collaboration with external organisations enables port managers to initiate resources sharing networks with the objectives of increasing capabilities and capacities, while reducing individual organisational costs, and developing commonalities in disruption management resources (Haraguchi, Lall & Watanabe 2016).

In relation to port resilience and resource sharing between stakeholders, Heaver (2009, p. 8) observes that 'the most important driver of the willingness of members of the port community to work together is the existence of external threats'. Personnel are an important resource in port risk management. Resilience practices such as cross training and multi-skilling as many personnel as possible, and ability to call upon experienced contract labour, assists an organization to become more operationally resilient to personnel absences, as might occur with pandemics (Carralli 2006; McDonald *et al*. 2018). In addition, vulnerability analyses should be conducted for both internal and external potential points of failure, and when engaging with external goods and services providers, a port should establish emergency management relationships, collaboration, communications, redundancies and resources sharing (AG 2016). External communication and collaboration involves shared exercises and dissemination of lessons learned, plus maintenance of exercise and actual disruption records.

Resilience learnings and knowledge are an important port resource when resilience capabilities are needed. For example, port operations are dependent upon the timely availability of external resources, and simple acquired knowledge such as current checklists of names, roles and contact details of external stakeholders becomes critical when external assistance is required (AG 2016).

Pelling (2011) characterises resilience learnings in three categories, the first of which involves managers learning to cope with adversity and improving their organisational processes. The second category of resilience learning is associated with adaptation to adversity and changing processes to meet corporate objectives. The third type of learning is characterised as transformational, for example in relation to when a port's operational environment is altered, and in response the

port's goals and objectives must correspondingly be changed. This third type of learning involves recognising when a port is approaching or is passing a 'tipping point' where the port is transposed from a stable set of operating circumstances to another state through natural or human-caused disruption (explained further in S 5.2.1). In this disruptive situation, management is required to manage, recover, and adapt or transform to an altered state of operations (Nelson, Adger & Brown 2007; Fisher 2011). An essential form of resilience learning involves methods for developing situational awareness, which requires port managers to develop a clear understanding and knowledge of their port's internal and external operating environments, sufficient to anticipate when circumstances are changing (Farjoun 2010; Weick & Sutcliffe 2015).

Generic resilience frameworks (BS 6500:2014; ISO 22316:2017) provide scant guidance on how to operationalise resilience theory into port management practice. A further gap in the knowledge exists with little known about Australian port managers' risk and resilience learnings and qualifications, and consequently whether their levels of knowledge are sufficient to operationalise resilience theory into practice. Accordingly, empirical research is required to better understand port performance measurement and management systems in relation to risks. Assisting port managers to better understand resilience, and their organisational progress resilience towards higher levels of resilience, might be accomplished with the availability of resilience capability maturity models, which are now discussed.

5.8. Establishing a port resilience maturity model

There appears to be little guidance for port managers who wish to understand the processes involved in building resilience within their organisation, and what needs to be planned for in the contexts of time, cost and resources. The ISO 2316:2017 resilience standard provides port managers with information that, when coupled with learnings and guidance from elsewhere, might be translated into a fit for purpose resilience capability maturity model, shaped to reflect individual port characteristics and circumstances. The purposes of a maturity model include assisting organisations to manage within the subject area, and to measure their organisational progress in improving or maintaining levels of competency (Bititci

et al. 2015). With the emergence of literature that focuses upon organisational resilience indicators including those of ports (Brown, Seville & Vargo 2017), a proposed port resilience management maturity model appears to be timely.

Maturity models are closely associated with resilience frameworks like the conceptual resilience implementation framework discussed in the previous section. A focused resilience framework might provide similar information and processes to those within a resilience maturity model, and a detailed maturity model likely carries an embedded resilience framework (Caralli, Knight & Montgomery 2012). A maturity model helps to identify any resilience shortfalls, establish performance attainment targets, and assess potential vulnerabilities to disruption (Cockram & Van Den Heuvel 2012; Miklosik 2015). Additionally, maturity models outline performance management system requirements, indicate targets for resilience performance and capabilities, and are a basis for review/audit of present circumstances (Melnyk *et al*. 2014).

A format for a port resilience maturity model is suggested by the risk management standard (ISO 31000:2018) as discussed in Chapter 4 and the importance of using a capability maturity model is because such models might:

a) be employed in multi-dimensional contexts;
b) measure conditions conducive to enabling resilience from successive stages between minimal preparedness to optimal performance;
c) provide a strategic plan for progressively building port resilience (Crawford 2006; Gibson & Tarrant 2010; Bititci *et al.* 2012); and
d) be relatively simple to adapt for both academic and practitioner purposes (Chapman 2011).

Maturity model performance measurement and management systems reportedly arose from early information systems management research by Nolan and Gibson (1974). Conceptually, capability maturity models typically consist of four scales to describe maturity progress that encompass initiation, expansion, formalisation and maturity stages of implementation. When translated into a contemporary port resilience format, this equates to:

a) operationalisation of resilience theory into practice, and initiation of the resilience-building process;
b) Board mandate (expansion of the resilience process across the organisation);
c) emergent capabilities and leadership (formalisation of port resilience strategies, plans and concepts); and
d) advanced and effective resilience capabilities and capacities (maturity level).

Gibson and Tarrant (2010) outline an evolutionary progression of resilience attributes, performance capabilities, characteristics and indicators for depicting maturity levels of resilience. These are adapted towards a proposed port resilience implementation maturity model (Figure 5-4) that that forms a blueprint for building port resilience. This model provides benchmarks to indicate the port's present resilience level and status, and indicates what attributes and capabilities are required in further building or enhancing levels of resilience (Carralli, Knight & Montgomery 2012). A capability level is achieved when port managers achieve a nominated milestone and can perform specified activities at a consistent and predictable level of competence (Bititci *et al*. 2015; Proença *et al*. 2017).

This port resilience maturity model provides an organisational pathway from an unprepared state of low resilience through successively more systematic and better managed states to a set of advanced and effective resilience capabilities (Wendler 2012). The commencement of the model (Level 1) reflects a port's organisational compliance with ISO 31000:2018 since resilience is constructed upon and enhances traditional risk management tools and capabilities (Van der Vegt *et al*. 2015). Sequential steps provide a means of assessing the port's ascending levels of potential organizational resilience, to assist managers in identifying their port resilience strengths and weaknesses (Wendel 2012, 2014).

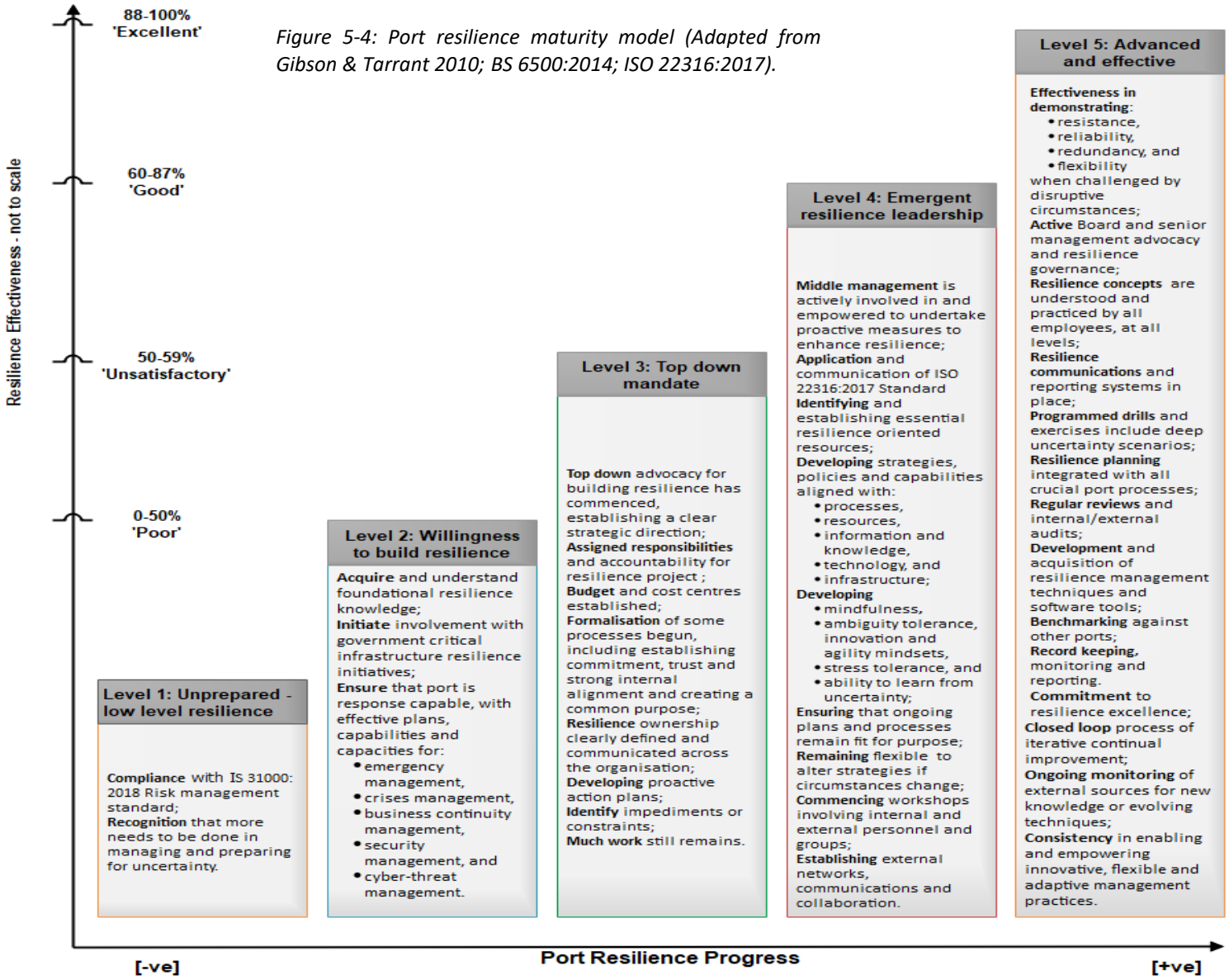


Figure 5-4: Port resilience maturity model (Adapted from Gibson & Tarrant 2010; BS 6500:2014; ISO 22316:2017).

The model also provides guidance for what enhancing actions and supporting tools might potentially lead to resilience improvement (Wendel 2014). Resilience indicators, enhancing actions and supporting tools that are employed in this model are suggested by:

a) Labaka-Zubieta (2013) – resilience plans and policies;
b) Berkes (2017) – socio-ecological resilience qualities and collaboration;
c) BS 6500:2014 and ISO2316: 2017 – generic resilience indicators and factors;
d) Häring *et al*. (2017) – resilience management processes;
e) Southwick *et al*. (2017) – leadership;
f) OECD (2017) – innovative risk governance; and
g) Oliva & Lazzeretti (2017) – port adaptation to disruption.

To the best of the researcher's knowledge this is the first time that a port resilience implementation blueprint has been attempted in the literature. The proposed port resilience implementation maturity model was materially adapted from the literature to reflect the port resilience context. The layout and development of the resilience maturity model was based on that used in Section 4.8, the proposed risk maturity model. In Figure 5-4, the y-axis scale for port resilience effectiveness was modified from groupings that were suggested by Brown, Seville and Vargo (2017) in their survey of New Zealand organisational resilience effectiveness. Conceptually, the resilience maturity model may be of use to academics and practitioners in advancing critical infrastructure resilience concepts and placing these concepts in use.

5.9. Summary

Australian ports are integral elements of the strategically and economically important national critical infrastructure system, and Australian government initiatives actively encourage critical infrastructure managers to enhance their organisational levels of resilience. Little is known about resilience as practiced by Australian port managers, and research into this topic appears to be timely.

Chapter 5 extensively investigated the state of organisational resilience knowledge and its relevance to ports, and identified gaps in the knowledge concerning what influences, drivers and impediments might affect the operationalisation and enhancement of Australian port resilience. A New Zealand study for example, found that some critical infrastructure managers are reluctant to break down silo management practices, and are unwilling to conduct emergency and business continuity exercises and drills (Brown, Seville & Vargo 2017). Chapter 5 also indicated where further research might lead to clearer resilience understandings for both academics and practitioners.

Indicators of organisational resilience were sourced from the literature and applied to the port situation. The resultant discussion outlines fundamental resilience information regarding the associations between enterprise risk management, emergency management, business continuity and resilience. Resilience was found to be a valuable port management adjunct to conventional risk management and business continuity techniques, enabling managers to absorb and manage new, emerging, complex and unpredictable risks to port operations. The literature suggests that resilience effectiveness towards new, unpredictable and unexpected risks relies upon adaptive and innovative management interactions with an unfolding and changing risk environment. There is little resilience education to provide specific guidance for what managers should do for every type of disruption, rather academia provides guidance towards how managers might evolve resilience capabilities and become empowered to exercise ad hoc solutions to unconventional hazards.

Further contributions are made towards building resilience within the port's operational business continuity strategies, methods and processes through the drafting of a resilience implementation framework. The framework was compiled from the literature, plus guidance from international standards BS 65000:2014 and ISO 22316:2017 - Security and resilience. This framework (shown in Sub-section 5.5.4) also assisted in the compilation of a proposed resilience maturity model by which port managers might establish how far their resilience practices have

evolved, and what next steps are required to further improve their resilience competencies.

The proposed resilience maturity model that suggests guidelines for implementing port resilience was adapted from existing resilience models and is conceptually a 'follow-on' to the ISO 31000:2018 risk management framework. Information identified in compiling the resilience maturity model assisted in forming survey questions for the empirical components of this study. The following Chapter 6 presents the quantitative and qualitative methodology employed in addressing the research problem.

Chapter 6: Research methodology

6.1. Introduction

The preceding chapters provided foundational knowledge towards the research problem and investigated the literature for information that sheds more light upon the investigation. The literature review described the port and port operations characteristics, port hazards and vulnerabilities, the tenets of conventional risk management, and principles of organisational resilience and how it might relate to ports. However, the literature review revealed that there has been minimal discussion about Australian port risk management abilities to cope with high consequence disruptions and how effectively managers might maintain business continuity. Resilience studies related to Australian ports largely overlook operational resilience, and managers' roles and capabilities in operationalising resilience at their ports.

Chapter 6 describes the research methodology to be employed in answering the research questions. Specifically, it identifies the type of empirical study and its participants, its procedures, and the chosen data analysis approach (Rudestan & Newton 2015). Data analysis techniques are discussed, and research administration including ethical considerations and research quality controls is summarised. The chapter describes the methodological approach taken in reaching a clearer understanding of Australian port risk management and resilience effectiveness. It begins by outlining the research objectives.

6.2. Research objectives

Research methodology is defined as: '…the philosophical stance or worldview that underlies and informs the style of research. It could be termed the philosophy of methods' (Jupp 2006, p. 175). Research methodology refers to the general strategy and logic framework upon which research and research design is constructed, and in this chapter the chosen methodology is explained in sufficient detail so that the research outcomes might be evaluated and/or replicated (Bryman 2015). Objectives in formulating research methodology (Garg & Kothari 2014; Christensen, Johnson & Turner 2015) are to:

a) systematically investigate and formulate the research problem;
b) explain the approach and theoretical stance taken and why others are excluded;
c) establish what constitutes the survey population and sample; and,
d) to establish how data collection and analysis is to be undertaken.

The primary objective of this thesis is to establish a clearer understanding of how the dynamics of disruptive change are managed within the contemporary Australian port's risk management capabilities and processes (Haraguchi & Kim 2014; Haraguchi, Lall & Watanabe 2016; Davidson *et al.* 2016). Specific thesis objectives are to:

a) investigate demographics of the Australian port senior management population;
b) explore port risk management and resilience mindsets and competencies;
c) identify distinguishing characteristics of the port risk environment (past and predicted);
d) explore opportunities for resilience changes that might transform and reconfigure port disruption management capabilities and capacities to higher levels; and,
e) examine how resilience concepts might be further operationalised at Australian ports.

The research questions as discussed in Chapter 1 were drafted to provide a clearer understanding of what processes and mechanisms of port resilience are required to counter unexpected disruptions. For convenience, the research questions are provided below:

PRQ: How does the port as a crucial networked component of the complex critical infrastructure system manage the risks and outcomes of regional disruptions?

SRQ1: How do ports currently manage risks and unknown unknowns arising from disruptive events?

SRQ2: What do ports need to change in their practices to become more resilient? and

SRQ3: How might ports operationalise resilience to best manage/overcome risks and unknown unknowns arising from disruptive events?

The literature review found few examples of research, theory and guidance that is directly relevant to Australian port resilience, despite the Australian government's determination of ports' importance as both critical infrastructure (AG 2015), and their crucial associations with supply chain risk management (Christopher 2016; Polemi & Papastergiou 2017). This thesis contributes to the knowledge by undertaking survey and data analysis involving senior port managers across Australia's 21 port authorities and 6 State government marine authorities (Ports 2017). Australian ports are important components of Australia's critical infrastructure (AG 2010) which leads the thesis towards a systems method approach, because resilience is a holistic property of critical infrastructure systems (Gopalakrishnan & Peeta 2010). Disruption management and recovery cannot accurately be conceptualised in terms of any one organisation, one network or even one system, because each critical infrastructure sector is reliant upon and interdependent of others (Hsieh, Tai & Lee 2014). From a resilience operalisation perspective, these resilience and systems theory approaches are further aligned with dynamic capabilities theory to provide increased insights into how Australian ports might build their levels of resilience (Teece 2018).

In alignment with the thesis objectives, this research design is conceptualised as being:

a) exploratory in formulating new theories and in contributing to the pool of critical infrastructure resilience knowledge;
b) explanatory in establishing new evidence of present and past port-systemic resilience attributes; and,
c) generalisable in contributing new knowledge towards improving or modifying port critical infrastructure resilience to future disruptions.

As will be discussed further, data for this study will be gathered from selected research participants by a cross-sectional process, over a length of time approved by the University of Tasmania's Ethics Committee.

6.3. Research population and sample size

An important preliminary research step is to identify the target population, from which survey research draws on a sample to generate generalisations about attitudes and behaviour back to the population (Christensen, Johnson & Turner 2015). In this research, the population consists of port-centric senior executives with risk management decision-making roles and responsibilities.

6.3.1. Australian port management pool

The Australian port management population itself is small. From a port authority context there are 21 authorities and corporations, and six State government departments that are tasked with oversight of Australian ports. Examination of port authority web sites provides an indication of management size from their organisation charts. Each is overseen by a CEO, with between seven and nine senior managers managing departments or sections of the business. Government instrumentalities may be smaller, since their role is more focused on regulatory matters, safety and risk management. The Victorian Ports Corporation, for example, has a CEO plus senior executive team of three, while Flinders Ports (a privately-owned port operator in South Australia) has a General Manager and four senior managers (information was derived from respective web sites).

A sampling quandary arose from the small population of senior managers who are the decision-makers for their respective port organisations, with only some permitted to be spokespersons for their respective organisations (Lewis 2017). The population frame became a potential maximum of 54 managers, a figure derived from 27 organisations with up to two managers with delegated authority by their Board to act as corporate spokespersons for external queries, inclusive of survey responses (Gray 2017; Lewis 2017).

6.3.2. Port management population characteristics

Sampling in this research involved selecting sets of managers from the wider port executive population with decision-making responsibilities for risk and resilience management. This process is termed purposive sampling, and this involves a relatively small number of respondents to gather as much information in depth as possible about a phenomenon. Purposive sampling (Christensen, Johnson & Turner 2015, p. 509) occurs when the researcher**: '…**specifies the characteristics of the population of interest and then locates individuals who have those characteristics'. An alternative is probability sampling which seeks breadth of information from many respondents to gain representativeness of the entire population (Teddlie & Yu 2007; Patton 2015).

Purposive (judgement) sampling was employed in this research because of the researcher's judgement that:

a) the sample candidates are inherently homogenous in their fields of occupation, job descriptions, work experiences and regulatory structures;
b) they all rely on similar port-centric regional support systems; and,
c) all are challenged by similar new and emerging low probability/high consequence risks.

The invited senior managers are decision-makers within Australian ports, and in another type of investigation might be chosen as Delphi research 'experts' capable of providing accurate information within their narrow field of practice (Thellesen *et al.* 2015). The study population included high level, authoritative professionals of CEO and senior management levels, who are accustomed to acting as spokespersons for their port-centric organisation. Their senior executive positions coupled with experience (time in senior management roles) were indicative of their abilities to understand concepts enunciated within the survey. Participation of senior decision-making managers was also intended to optimise data dependability in answer to the research questions.

The target population for this study was initially intended to encompass a more statistically meaningful number of participants, which necessarily required multiple informants from each responding organisation. However, personal

communications (Gray 2017; Lewis 2017) advised that port authorities typically place restrictions on the number of managers who are authorised to respond to external communications and permitted to speak on the 'corporate view'. The port CEO (according to Lewis 2017) customarily delegates authority for signing and/or releasing external correspondence to members of the executive team, inclusive of surveys, where usually only the CEO might provide this 'corporate view' (Lewis 2017). Within this widely-adopted delegation policy, port organisations establish a correspondence delegation document, authorised by the Chairman, and the extent of authorisations for releasing external correspondence depends largely upon the organisation's risk appetite (Lewis 2017).

6.3.3. Sample size

The sampling plan describes how this research approached the matter of selecting a sample from the port senior management population, what sample size was deemed to be adequate, and how the survey was administered (Glasow 2005). Bartlett, Kotrlik and Higgins (2001, p. 43) describe how inadequate or inappropriate sample size might adversely affect research quality, reliability and accuracy. They describe sample size as a factor that can either assist or impede researcher capabilities in detecting '…significant differences, relationships or interactions' within the research population'. Cochran (1977) argues that an unnecessarily large sample is wasteful, a minimalist sample size reduces quality of results, and somewhere in between, the sample size is just right. With these factors in mind, researchers generally calculate a minimum sample size to avoid having to work with too few responses, an outcome unsuited to statistical calculations and/or unfit for generalisability (Bartlett, Kotrlik & Higgins 2001).

Consideration towards sample size took considerable time to resolve, in recognition of Marshall *et al.* (2013, p. 11) advice that:

> Other than selecting a research topic and appropriate research design, no other research task is more fundamental to creating credible research than obtaining an adequate sample.

A problem for this research is that the Australian port management population could not provide a sample size that remains useful for generalisability. Fowler (2014) notes that there is no commonly accepted minimum survey response rate but advises that levels of non-response should be clearly explained should the number of completed responses be low. This implies that sample size is a matter for researcher judgement, as argued by Hoinville and Jowell (1985, p. 73):

> In practice, the complexity of the competing factors of resources and accuracy means that the decision on sample size tends to be based on experience and good judgement rather than relying on a strict mathematical formula.

The mixed method approach employed in this thesis envisaged a primarily quantitative analysis of survey responses, hence the concern for attaining a sample size sufficient for statistical soundness (Pallant 2016). Regardless of any mathematically derived ideal figure for survey respondents, the sampling was restricted to those managers to whom email access was available, and who were both authorised and willing to respond. Homogeneity of the senior executive levels of port management excluded the requirement for stratification and clustering, and so a smaller sample size was judged to become more acceptable. A further and important consideration towards sample size is the purposive selection of survey participants.

For completeness of sample size estimates, the researcher reviewed qualitative sampling techniques. Within mixed method research the quantitative sample size is commonly much larger than the qualitative segment (Teddlie & Tashakkori 2009). Academic advice that purposive mixed method sample size is typically of 30 respondents aligns with the findings of Marshall *et al.* (2013) whose literature review examines 83 qualitative studies from five top ranking journals to establish sample size rigor in qualitative data generation. Few of these studies justified their sample size, but from those that did, Marshall *et al.* (2013) conclude that grounded theory qualitative studies should aim towards 20-30 respondents.

Recognition was made early in this thesis that the survey response rate would likely be low, not only because response rates are progressively declining (Petroni *et al.* 2004; Curtin, Presser & Singer 2005; Wagner 2008) but because a major limitation on respondent numbers is imposed by the small size of the Australian senior port management executive population, reduced further by limitations on the number of managers who are authorised to become organisational spokespersons (Lewis 2017). Within the academic literature, emphasis is placed upon gaining high response numbers to a survey by expanding the population, however this is a factor related to the statistical rigour of studies. Rarely addressed is another component of research probity, which is to gain quality in results, rather than quantity. For example, Rice and Trepte (2012) undertook a port resilience survey and expanded their global survey population to include shippers, carriers, services providers, freight forwarders and other third parties not directly involved in port emergency management and resilience capabilities. Of the 525 respondents to their survey, only 44 were representatives of port authorities. Potentially, the Rice and Trepte (2012) survey findings were exposed to selection bias (respondents not representative of the population of interest) or ignorance bias (respondents knowing little about the subject under survey) which suggests that bigger is not always better.

For this thesis research, the size of the senior port executive population limits the potential number of respondents, but a restricted sample size is not regarded as an indicator of poor data quality – rather it is recognised as a limitation of statistical relevance.

6.3.3.1. Sampling methodologies in other port resilience studies

The literature review indicated a paucity of Australian port resilience studies, other than discussions on the relationships between port resilience and climate change. Of interest, an aviation-oriented study by Wood, Dannatt and Marshall (2006) investigating airline resilience on behalf of the Australian Transport Safety Bureau found that their resilience research problem lacked previous research precedents. This led them to select data gathering and analysis methodology

suited to ‘real organisations with real and relevant issues’ (p. 7). Their sampling frame was small, consisting of eleven airlines and thirty-two managers authorised to speak from a corporate perspective. Based on the preliminary findings and assumptions arising from their literature review, the researchers employed a modified case study approach, which they analysed using qualitative and quantitative software programs. Thirty-two interviewees contributed to the primary sequential qualitative phase, and eleven participants from these qualitative interviews formed the quantitative phase sample. Acknowledged limitations of this first exploratory Australian airline resilience study included low levels of representativeness and generalisability. The small quantitative phase sample size (n = 11) was partially attributed to the ‘…often highly confidential nature of the data’ plus respondents’ concerns for protecting their corporate reputation for safety (Wood, Dannat & Marshall 2006, p. 8). A possibility arises that similar but unreported confidentiality and reputational concerns may influence this thesis research.

As discussed in Subsection 6.3.3, a web-based global survey with a similar research problem to this study was conducted by Rice and Trepte (2012). The research was conducted from a port resilience perspective for the Massachusetts Institute of Technology (MIT) Center for Transportation and Logistics and comprised a literature review followed by a web-based survey of managers related to ports. The MIT research aim was to gather a general understanding of managers’ port disruption experiences, and to gauge their opinions on operationalising port resilience. Rice and Trepte (2012) employed multiple data analysis techniques, including Structural Equation Modelling (Kline 2016; Hox, Moerbeek & van de Schoot 2017) and the use of exploratory factor analysis. Rice and Trepte (2012) collected 525 survey responses from non-probability convenience-based sampling, and their management respondents include port authorities, terminal operators, shippers, carriers, services providers, freight forwarders, consultants and other third parties.

The Rice and Trepte (2012) survey response exceeds the minimum survey sample size of 100 respondents recommended by Kline (2016) for SEM. Some factors from

the Rice and Trepte (2012) study were examined for usefulness in formulating survey questions for this thesis, however, the small sampling frame represented by Australian port managers (Ports 2017) impedes the use of an SEM research approach.

This thesis focuses upon port authority managers' risk management and resilience abilities to cope with disruption. The port's intermodal business continuity is more directly associated with port authority management and staff than with external third-party shippers, carriers and freight forwarders for emergency management planning, responses, controls and competency measures (Bichou, Bell & Evans 2014; Burns 2015). Rice and Trepte (2012) recognise this jurisdictional issue, in questioning whether port resilience is a matter of port authority or terminal operator responsibility, or whether port resilience is a responsibility of the wider port operations community. Rice and Trepte (2012, p. 8) circumvent this issue by researching resilience of the broader 'port environment', which they define to mean as either '…an individual port, a regional set of ports, the ports in a single state, or the collective ports across the country'. Nevertheless, their findings constitute a useful foundational study for further, more focussed port resilience research.

The American Association of Port Authorities (AAPA) endorsed a study towards creating a port resilience index (Morris & Sempier 2016). Their data collection methodology consists of a Delphi Method evaluation of expert opinions (n = 13) which is then assessed by qualitative means. The findings from this research were tested in three pilot studies and then in subsequent case studies involving three Gulf of Mexico ports. The subsequent self-test resilience index became a standard for the AAPA ports.

Omer (2013) addresses the research question: How can the resilience of networked infrastructure systems be measured? Omer (2013) investigates multiple segments of global critical infrastructure systems, including a maritime transportation segment that involves two Pacific ports. The research employs a case study approach with qualitative and quantitative analysis techniques to establish port resilience indicators from a shippers' perspective. However, the

port-centric component of Omer's research is small, and Omer's greater contribution is towards a wider study of global transportation and logistics.

Examples of contemporary port resilience studies include Achuthan (University College, London) who is investigating simulation models to assess the resilience of port systems (Shaw, Grainger & Achuthan 2017), and Morris (Louisiana State University) who recently completed a study to develop a qualitative resilience assessment tool for US Gulf ports (Morris 2017).

6.4. Theoretical framework

In approaching this research within a largely unexplored field of interest, and to better understand the research dynamics, the researcher examined the literature for thoughts, concepts, assumptions and beliefs that are related to the research questions. The findings are arranged into a cohesive order by means of conceptual port risk and resilience frameworks (Figures 4-1 and 5-3), and port risk and resilience maturity models (Figures 4-3 and 5-4). These tools were created from multiple academic sources, to illustrate the types of strategies, plans, processes and techniques that are considered necessary to support port risk and resilience management.

Theoretical frameworks, according to Ravitch and Riggan (2016) are foundational to drafting the research questions, where constructing a bounded framework assists in reducing extraneous data that might impede the analysis, while retaining factors that might benefit from data comparison. The theoretical frameworks created to guide this thesis' empirical research are firmly grounded in the literature review findings (Maxwell 2013). The surveyed literature is founded upon multiple theories and approaches not always related to port risk management, to ascertain whether new connections or concepts might be established. Conceptual models can be employed as an organising planning tool in empirical research involving working hypotheses in exploratory research (Shields & Rangarajan 2013). For example, Kasperson *et al.* (1988) employ a conceptual model in systematically linking a technical assessment of risk with organisational and societal perspectives of risk perception and risk-related behaviour. From the perspective of this thesis,

Kasperson *et al.* (1988) present an argument that the differences between technical/objective (evidence-based) perceptions of risk) and subjective/societal (values-based) perceptions of risk can lead to disproportionate response to minor risks of low consequence following subjective evaluations, while major risks might go unremarked. The design of an effective conceptual port risk management framework should therefore take this possibility of societal bias into consideration.

The advice of Dewey (1938) although dated, authoritatively argues that exploratory research requires direction in its data collection and analysis phases through what he interchangeably describes as 'working hypotheses', 'blueprints', 'maps', and 'conceptual frameworks'. Dewey (1938, p. 169) argues that 'blueprints and maps are propositions and they exemplify what is to be propositional'. Mapping hypothetical interrelationships between concepts and statements enables the researcher to demonstrate how his/her investigation dovetails with the existing field of theory and research, and how the research might contribute to knowledge (Creswell & Creswell 2017; Ary *et al.* 2018).

This research builds upon findings from the literature review to make logical sense of how ports might manage disruptions, what processes and outcomes result when these adverse events occur, and how disruption consequences are modified by systemic resilience. Whether the port can maintain its required operational capabilities consequent to disruption (or be able to recover within a tolerable time) is hypothesised to be dependent upon port risk management and resilience effectiveness, and port business continuity closely coupled with similar attributes from crucial goods and services providers. The consequences of a disruption might impact and ripple across the port system, and its effects ultimately felt outside the port (for example, by supply chains, government, regional businesses and community). Minimisation of disruption consequences and cascading potential is hypothesised to be dependent upon the port system's risk management and resilience competencies, as described in the literature review. The actual state of competencies for Australian ports is unknown, which lends direction and importance to this research and its methods.

6.5. Research methods

Research can be performed within either quantitative, qualitative or combined approaches, depending upon which format works best. Quantitative research assumes a narrow field of focus, assuming a Descartian approach of reducing complex phenomena into manageable pieces for study and eventual reassembly into the whole, and for engaging in sequential and complete steps in the research process (Garber 2005; Cohen, Manion & Morrison 2013). Research emphasis is placed on the collection and analysis of numerical data, and Best and Kahn (2006, p. 118) argue that such findings might reveal:

> Conditions or relationships that exist; practices that prevail; beliefs, points of views, or attitudes that are held; processes that are going on; effects that are being felt; or trends that are developing.

Alternatively, qualitative research adheres to a variety of interpretive research methodologies in developing theory and explaining human interactions from data analysis, an approach that leads more to understanding the phenomena rather than explanation (Glaser & Strauss 1967; Charmaz 2006; Creswell 2009). Theory is grounded in the data and emerges from the data analysis (Lincoln & Guba 1985). In this context, researcher influences upon the study outcomes, rather than forming a study limitation, are regarded as holistic knowledge inputs towards analysis and exploration of the phenomenon (phenomenology). The researcher attempts to gain richer access to the knowledge and understanding than may be possible through alternative narrow and calculated empirical findings. This process is abetted by the researcher's understanding that a scientific reason for an event or outcome might differ from a real world 'practical' reason (Ormston *et al.* 2014; Nardi 2018).

In considering what methodology and techniques to undertake for this study, the researcher assessed multiple approaches including case studies, qualitative immersion, and surveys in their various forms. Case studies are often employed in disaster-related investigations (Coleman 2004) - for example the Bali bombings (Royds, Lewis & Taylor 2005); Hurricane impacts on the US eastern seaboard

(Becker *et al.* 2015; Haraguchi & Kim 2014); seaport resilience assessments (Liu 2014; Becker & Caldwell 2015); and, disasters of human causality (Chernov & Sornette 2016). Persuasive outcomes from case study methodology require investigations of port risk management attributes within a variety of contexts, or more beneficially, observations involving the port in either managing, or simulating a specific disruption scenario (Yin 2013; Bryman 2015). Case studies share some aspects of mixed methods research, in analysing both qualitative and quantitative data from in-depth interviews and questionnaires (Christensen, Johnson & Turner 2015). Hodkinson and Hodkinson (2001) argue that case studies demonstrate some important limitations, for example, inapplicability to many research questions, potential for researcher subjectivity, typically small sample sizes, constraints in quantifying the findings, poor generalisability, time consuming and expensive, and eventual findings are easy to dismiss if research outcomes are unfavourable. For this thesis, other research methods were considered to find techniques that avoid the restraints imposed by case study methodology.

Narrow ethnographic observations of a few selected ports, their management activities and processes at work, work-place interviews and focus groups were considered for deriving insights into managers' understandings of the phenomena, and for indications of their risk-related behaviour (Bryman 2015). The primary consideration against ethnographic observations related to potentially wider benefits in investigating multiple ports for diversities of opinion, and to source research data from multiple geographic regions with varying climatic hazards. A secondary limitation of ethnographic observations is that like case studies, these achieve deep understandings of a few management teams under observation, at the expense of gaining a more holistic perspective.

Survey methodology (for example web-based surveys or telephone interviews) is a further means of gathering data, following the pragmatic argument of Goodwin (2010, p. 463) that:

> Survey research is based on the simple idea that if you want to find out what people think about some topic, just ask them. That is, a survey is a structured

set of questions or statements given to a group of people to measure their attitudes, beliefs, values, or tendencies to act.

Survey types in a social research context are described by de Vaus (2014) as face-to-face, phone, postal, email, disk by mail questionnaires, and web-based self-administered questionnaires. As explained in the following section, after due consideration this research employed self-administered web-based survey methodology. Phone surveys were considered, but the researcher had extensive personal acquaintances within the potential respondent population and a possibility existed for surveyor bias to be introduced.

6.6. Data gathering and analysis considerations

As this research is regarded as a preliminary investigation into Australian port resilience, where research is immature, and the field is largely under-studied, data gathering becomes an exploratory process. Beins and McCarthy (2012) advise that surveys are a widely used and accepted form of data gathering in contemporary social science and business research, and this technique is adaptable to explanatory, descriptive, and exploratory research approaches (Neuman 2014). Analysis of data can be performed quantitatively, qualitatively or by the process of exploratory mixed method research design (Creswell 2013). Mixed methods research involves a '…combination of quantitative and qualitative research techniques, methods, approaches, concepts or language into a single study (Johnson & Onwuegbuzie 2004). It is an inclusive process, which incorporates inductive (identification of patterns), deductive (testing of hypotheses) and abductive (finding a 'best fit' for explanations of results).

6.6.1. Mixed method approach

Data analysis using mixed method research was considered due to its properties in potentially contributing new knowledge and perspectives on the research topic through the concurrent and sequential use of words and numbers (Zikmund *et al*. 2013; Bazely 2009). The advantages are iterated by Marshall and Rossman (2014) who argue that a mixed methods approach increases validity for a topic that is little explored, as is the case with this research problem, and provides opportunity

to reflect the participants' context and points of view. Driscoll *et al*. (2007) argue that mixed methods research designs are a pragmatic solution to complex exploratory research, where qualitative data leads to a deep understanding of survey responses, while statistical investigation reveals patterns within the responses.

Mixed methodology (quantitative/qualitative) is useful for comparing and combining parallel information from diverse sources, discovering new insights from or discarding paradoxes and contradictions, and sourcing complementary and contrasting information between source types to explain a set of phenomena, even if separately, each item of information is only minimally useful (Bazely 2017). Mixed method studies are also useful in exploratory investigations for which robust conceptual and empirical foundations are immature (Brannen 2017). This approach permits both inductive and deductive reasoning, and the investigation of multiple types of data (Bryman 2015; Sekaran & Bougie 2016). When a qualitative phase begins first as a subordinate process in providing useful knowledge towards the research topic, it aids the drafting of the quantitative survey and later understanding of the survey data (Harrison 2013; Creswell & Creswell 2017). Employment of multiple methods within a single research study facilitates the inclusiveness and generalisability of quantitative data and increases the analytic contextual nature of qualitative findings (Sekaran & Bougie 2016; Creswell 2014).

Limitations of a mixed methods approach (Driscoll *et al.* 2007) are that amalgamating qualitative and quantitative data for analysis and assessment can be time consuming. Care must be taken in maximising sample size, and respondents' time should be respected in the interviewing process. A mixed methods approach adds complexity to the research design, and the guidance of theoretical frameworks as discussed earlier in this chapter aid in gaining a clear understanding and integration of investigatory concepts (Bryman 2015; Sekaran & Bougie 2016). Other potential disadvantages of a mixed methods approach include:

a) the need to avoid a mind-set that becomes biased towards either quantitative or qualitative philosophical tenets (Ritchie & Lewis 2013);
b) additional time for two approaches rather than one, and potentially, added expense of a dual approach (Fraenkel, Wallen & Hyun 2012); and,
c) a mixed methods approach requires a broader scope of research knowledge and expertise than a purely quantitative or qualitative study (Creswell & Creswell 2017).

Within this thesis, the limitations of mixed methods research were recognised, and the negative aspects partially minimised by ensuring that qualitative components of this research were fewer than quantitative. The literature review provided guidance on what qualitative questions to ask within a primarily quantitative survey questionnaire. The survey and its questionnaire were designed as a single-phase project, to permit concurrent qualitative and quantitative research questions, where one set of questions was not contingent on the other (Creswell 2014; Creswell & Creswell 2017).

6.6.2. Survey research techniques

Beins and McCarthy (2012) advise that surveys are a widely used and accepted form of data gathering in contemporary social science and business research. Survey research has its foundational roots in a positivist investigation approach, and this technique is adaptable to explanatory, descriptive, and exploratory research approaches (Neuman 2014).

Web-based surveys are increasingly utilised by researchers due to a growth in the population of professionals going online, technological advances that facilitate survey design, relatively low costs in administration, speed in data collection, an ability to monitor ongoing responses and response rates, ease of distributing reminders to non-respondents, media richness, and compatibility with analysis software (Simsek & Veiga 2001; Schutt 2012; Callegaro, Manfreda & Vehovar 2015). A surveyor can coordinate an e-mail message to participants (along with ethics-related information) to provide a direct link to the survey website (Callegaro, Manfreda & Vehovar 2015; Hewson & Stewart 2016).

Web-based surveys have inherent advantages compared with other survey modes. They can be deployed quickly at little cost, can shorten data-gathering times, and lead to faster survey results (Couper & Miller 2008; de Vaus 2014). These internet surveys do not unduly interfere with respondents' work responsibilities and commitments since the surveys can be completed at the respondents' convenience on either office or home computers. The researcher conducts a web-based survey at arm's length and avoids bias from interviewer effects, for example those related to telephone or face-to-face interviews. With the use of contemporary software, completed surveys might be immediately logged, partially analysed and available to the researcher for further processing. Statistical analysis processing is aided by ability export survey data to the selected statistical or coding software (McPeake, Bateson & O'Neill 2014).

Also, with continual internet oversight of the survey, the surveyor will know with some certainty when follow-up reminder emails need to be sent, which may not be the case with postal surveys. The researcher will learn useful para-data information with web-based surveys, including how many respondents did or did not open the survey, those who completed all questions, those who partially completed the survey, and those who required reminders to respond. Telephone survey methodology will produce similar survey administration data but not to the same degree of detail and accuracy.

Although web-based surveys are easy and flexible for respondents to complete and can allow them to break from the survey process and return later, the use of this methodology does not necessarily lead to higher response rates (Couper & Miller 2008). The surveyor might not have an accurate email address list for potential participants, some potential respondents might have several email addresses and rarely check one or more of these for messages, and managers might have moved to another organisation and hence become ineligible to participate in the survey (Bryman & Bell 2015). McPeake, Bateson and O'Neill (2014) suggest that from a contact list compiled over the past twelve months, up to 10% of email invitations to participate might be returned as undeliverable. With web-based surveys that seek access to the general population, there would be

concern regarding non-response rates or inability to contact potential participants with useful information, but who do not have access to a computer or are computer illiterate (Bryman 2015). However, port senior executives are unlikely to fit this respondent category, and in weighing the advantages and disadvantages of web-based surveys, judgement was made to proceed with this approach.

The web-based research format chosen for this study searched for plausible answers to the research questions by:

a) utilising focused survey questions;
b) comparing the opinions of segmented demographic groups;
c) comparing port capabilities, capacities and risk management culture (ensuring confidentialities);
d) ascertaining whether understanding differences occur between different segments of port management, and,
e) testing the survey findings for potential utilisation by academic, regulatory and commercial audiences.

The online survey tool SurveyMonkey (SurveyMonkey.com) was utilised to create the survey questionnaire which was emailed to specific respondents. As described by Creswell (2009), the survey results were returned to the researcher for analysis in the form of descriptive statistics. SurveyMonkey is widely used by university researchers and journal authors, and its validity and reliability of scores is deemed sufficiently trustworthy to correlate with results gleaned by other methodologies (Symonds 2011; Wissman, Stone & Schuster 2012). Other online survey publishing tools were considered, such as Instant Survey however SurveyMonkey appeared to enjoy much wider scientific usage and acceptance.

6.7. Questionnaire design, testing and administration

A questionnaire is a respondent self-report data collection instrument for measuring individuals' opinions, attitudes, perceptions, knowledge and behaviour, plus ancillary demographic or other relevant data (Jupp 2006; Christensen, Johnson & Turner 2015). Questionnaire design was formatted around

the four research questions and the schematic followed within the literature review, namely:

a. the port risk environment;
b. port vulnerabilities to disruption;
c. port disruption management capabilities; and
d. the port's resilience capabilities.

Survey questions were designed by a process of moving from the broad concepts of the research questions, and the risk management and resilience concepts gathered from the literature review, to a more specific perspective of port risk management and resilience (de Vauss 2014). This process was aided by the previously discussed risk management and resilience frameworks and capability models (Chapters 4 and 5) which in turn gave rise to port risk management and resilience indicators around which the survey questions were drafted.

The questionnaire design comprised a self-administered web-based survey, a process where the survey instruments physically reside on a network server (Survey Monkey), and accessed through participants' Web browsers (Jansen, Corley & Jansen 2007). The survey design was framed against a mixed method, primarily quantitative, single mode approach in keeping with the population demographics analysis, plus interpretive uncertainties and 'unknown unknowns' of the research topic. Steps taken to improve data reliability include multiple-question formats (open and closed), direct connectivity of answers to the data base, ongoing electronic response checking, all contributing towards maintaining a level of confidentiality beyond that of face-to-face or telephone interviews, and paper surveys (Zikmund *et al.* 2013; Jansen, Corley & Jansen 2007). The study employed both monadic and comparative data scales and was based upon an organisational resilience survey tool developed by Lee, Vargo and Saville (2013). This survey tool was previously tested within New Zealand post-earthquake scenarios (Rotimi 2010; Jones 2015) and was shown to have capabilities for identifying resilience strengths and weaknesses, present resilience levels, and areas of strategic change towards resilience improvement.

Survey questions were arranged in a sequential flow to maintain interest (Brace 2018; Nardi 2018). The question sequence was aligned with those of the conceptual frameworks and models at Chapter 4 (port risk management) and Chapter 5 (port resilience). Questions were formatted in the following categories:

a) port manager demographics;
b) port disruptions;
c) disruption preparedness;
d) business continuity;
e) organisational resilience capabilities;
f) port resilience practices;
g) operationalising port resilience; and,
h) opportunity to provide additional comments.

6.7.1. Types of questions

Closed questions gave respondents either opportunity to choose among several potential answers, answer categories, or, according to either a frequency, importance or agreement scale (Siniscalco & Auriat 2005). Advantages of closed questions include fewer answer possibilities and therefore more quantifiable responses, easier and faster to answer, and more variables can be tested within a given time than with open-ended questions (Siniscalco & Auriat 2005; Bryman & Bell 2015; Brace 2018). Disadvantages include bias through 'guiding' respondents towards answers they might not have thought of, or respondents tending to tick the same numbered responses all the way through the survey (Siniscalco & Auriat 2005). The limited number of answers restrict in-depth answers and preclude respondent innovation or originality (Siniscalco & Auriat 2005), and, suggested answers might not match respondent opinions (Dawson 2009). In this thesis' questionnaire, bias was minimised by formatting closed questions differently to avoid repetitious patterns of answering, and creativity was encouraged by including comment boxes or an open-ended invitation for more detail (Siniscalco & Auriat 2005; Dillman, Smyth & Christian 2014; Brace 2018). Also, a 'don't know' or 'unsure' option was included to avoid participants providing artificial answer patterns if they did not know the answer (Dawson 2010).

Open-ended questions permitted free-form responses, in as much detail as the participant was prepared to give. Resulting in added richness of detail, deeper investigation and possibilities for sourcing new information, while disadvantages include the longer time taken to answer, greater thought required in the response, and researcher difficulties in coding or quantifying (Siniscalco & Auriat 2005; Dawson 2010). The questionnaire contains 36 questions and 71 sub-questions comprising 19 closed-ended questions, and 16 open-ended response boxes prompting free-form information or explanations intended to explore thoughts and concepts that might otherwise have been missed (Glasow 2005). Table 6-1 shows a breakdown of question types and numbers.

Survey category	**Question types and number of related questions**		
	Closed-ended	**Open-ended**	**Ranking**
Demographics	3	0	0
Disruptions – past and future	3	4	0
Disruption preparedness	3	4	0
Disruption responses	3	3	0
Disruption resilience capabilities	2	2	1
Resilience management	3	0	0
Operationalising resilience	2	2	0
Additional comments	0	1	0
Totals	**19**	**16**	**1**

Table 6-1: Disposition of question types within the survey (Author).

One question involved ranking responses in order. Question formats were varied across multiple choice, checkbox, rating scale, and ranking types, and where Likert Scale questions were used, respondents were given a choice of five answers, with an additional option of either 'not applicable' or 'unsure'.

6.7.2. Pretesting and units of analysis

This research investigates the phenomena of organisational resilience as it might be found in Australian ports, and hence the unit of analysis is port managers' perceptions as related to the research problem. To avoid the error of ecological fallacy (Jupp 2006) in making inferences about the entire organisation from one manager's response, the pool of participants is widened as far as the limited email

address database allowed. The pool of participants involved senior port risk management decision-makers, who are perceived to be capable and empowered to speak at a high level on the 'corporate view' (Pateman 2015). Recognition is made that these opinions will likely be shaded by differing port risk environments, plus individual manager's learnings and experiences (Rubin & Rubin 2005). Survey pretesting involved personnel from differing academic and practitioner backgrounds. Pretesting also assessed the survey question suitability in addressing the research questions and hypotheses, as shown in Table 6-2.

Links	**Independent variable**	**Dependent variable**	**Related survey questions**
PRQ - H1	Self-reported effectiveness of risk management behaviour	Ability to cope with disruptions	4, 9, 10, 14, 15
PRQ – H2	Recent encounters with disruptions	Increased acceptance of resilience concepts	5, 6, 9
PRQ – H3	Functionality of risk management resources	Increased business continuity capabilities	9, 13, 15, 16, 17, 18
SQ1 – H4	Risk environment mindfulness	Preparedness for new and emerging risks	11, 12, 13
SQ1 – H5	Vulnerability awareness	Reduction of uncertainty	4, 6, 7, 8, 12, 13
SQ1 – H6	New and emerging port risks	Vulnerability to business continuity failures	7, 8, 11, 12
SQ2 – H7	Leadership and collaboration	Resilience capabilities	14, 16, 17, 23, 24, 25
SQ2 – H8	Acceptance of resilience concepts	Enhanced resilience development	25, 28
SQ2 – H9	Transformational learning behaviour	Adaptiveness to change	4, 14, 15, 21, 23, 26
SQ2 – H10	Understanding drivers for risk management change	Improved resilience capabilities	8, 11, 12, 22
SQ3 – H11	Turbulent port risk environment	Reduced ability to operationalise resilience learnings	5, 6, 7, 10, 11, 12
SQ3 – H12	Conceptual understandings of resilience indicators	Meaningful application of theory to management capabilities	19, 20, 21, 22, 26, 27
SQ3 – H13	Resilience advocacy in strategies and plans	Heightened resilience performance	21, 23,26
SQ3 – H12	Resilience performance objectives	Measuring and benchmarking resilience implementation	26, 27, 28

Table 6-2: Links between research questions, hypotheses and survey questions (Author).

6.8. Survey pretesting outcomes

Survey pretesting is a process recommended to evaluate whether a questionnaire has potential to create problems for interviewers or respondents (Presser *et al*. 2004; Dillman *et al.* 2014). The purposes of pretesting (Dawson 2010) include:

a) discovery of ethical issues previously overlooked;
b) question appropriateness to the research problem;
c) a check that measurement levels in questions are appropriate;
d) assists in population and sampling decisions; and,
e) provides a guide to questionnaire length and response times.

Accordingly, the survey instrument underwent pretesting as a precursor for the Ethics Committee submission and involved assistance from a panel of four academics and three high level industry participants known to be familiar with port crisis management through research network contacts, inclusive of academia. The pre-test group was requested to comment on whether the questions were clear, reasonable, logical, interesting and appropriate (Siniscalco & Auriat 2005; Dawson 2010). They were also asked whether the instructions were clear, relevant and logical. Comments were received on survey design and completeness, question inclusivity and suitability, the survey framework, and the panel members' impressions on the survey user-friendliness (Presser *et al*. 2004; Krosnick 2018). Results of pretesting were regarded as preliminary outcomes, garnered primarily to assist in modifying (if necessary) the design of the ultimate study. Prior to pretesting, a fellow researcher working in an allied resilience field provided a welcome sounding board for revising an early draft version of the questionnaire.

An informed consent form was inserted into the online survey questionnaire (Appendix C) and participants could only perform the survey if they clicked the 'I agree' icon to acknowledge the informed consent conditions. The survey was expected to take approximately 30 minutes to complete, as indicated during the pretesting phase and in the event, average completion time was 22 minutes and 5 seconds. However, this average completion time incorporated foreshortened and partially completed returns.

Feedback from the pre-test panel indicated that the SurveyMonkey instrument was easy to use, and no technical problems were encountered. The lengthy preamble was discussed; however, the preamble contents were required to comply with ethical standards and could not be shortened. One respondent later commented that he skipped 'the fine print'. This pretesting phase was beneficial to survey quality, with panel members providing essential feedback about the clarity, completeness, and appropriateness of the survey proforma and processes. Feedback responses indicated that with revision in some areas:

a. the questionnaire was suitable and appropriate for investigating the research problem;
b. that survey completion time was 30 minutes or less;
c. some rewording was required; and,
d. two further questions were required for completeness.

Changes also included rewording of two headings, shortening the initial questionnaire, and compliance with the pre-test panel's suggestions that several ambiguous or superfluous questions be removed (these actions accord with the advantages of pretesting reported by Siniscalco and Auriat, 2005, and, Dawson, 2010). Layout design and end of each section wording were adjusted to make the survey more user-friendly and to better encourage participants to respond through until completion (Rogelberg & Stanton 2007). A closed-ended question was found to have overlapping time categories, and these were altered to become mutually exclusive, while another question was amended to remove a double-negative effect (Christensen, Johnson & Turner 2015). Following the pre-testing process, and receipt of University of Tasmania Ethics Committee approval, the survey questionnaire was deployed and the data gathering proceeded for a period of ten weeks.

6.9. Survey analysis process

The quantitative and qualitative data sets to be acquired from the survey questionnaire were processed in the context of a mixed methods study (Creswell 2013). As suggested by Miles, Huberman and Saldana (2013) these processes

embodied data reduction, data display and conclusion drawing and verification. The survey framework lends itself to the use of Excel and SPSS assistance in assessing reliability, validity, and sensitivity. Comparative data analysis was applied to interpreting open ended questions and borrowed from learnings obtained during the literature review.

Computer assisted data management and interpretation were employed to assist in research reliability and replication capability (Ott & Longnecker 2016; Bazely 2017). Computer usage is increasingly relevant to scientific research and software advances provide improved visualisation of data in the form of graphs and charts, increased flexibility in coding and grouping decision making, and provide the researcher with vastly increased data storage and access capabilities (Rademaker, Grace & Curda 2012; Bazely 2017). According to Bazely (2017) qualitative data can readily be converted in a quantitative format with the use of off-the-shelf software, a procedure sometimes known as 'quantifying' (Ward 2007; Shemmings & Ellingsen 2012). This technique also lends itself to this thesis' data analysis processes.

6.9.1. Qualitative data analysis – Dedoose web-based software

The qualitative empirical research employed the generically named Computer Assisted/Aided Qualitative Data Analysis (CAQDAS) computer software to assist in qualitative data analysis. Several of the many QDAS programs that assist in qualitative data analysis and code-based theory building include NU*DIST, NVivo, Atlas.ti, Hyper-Research, and Dedoose. These software applications provide a contextual means of organising, filing and utilising large quantities of text-based data, usually by point and click coding, text search and storage, rapid cataloguing and indexing, and ready retrieval (Weitzman & Miles 1995; Bryman 2015). Importantly however, computer assisted data analysis requires a human contribution to perform the interpretive and intuitive assessments and decision making that are crucial to qualitative analytic research (Weitzman 1999). The literature was consulted to select an appropriate qualitative software package for this research.

Nielsen (2012) investigates the attributes of four QDAS programs as shown in Table 6-3. The online software application Dedoose was seen to possess comparative advantages that might contribute more rigour to PHD research, however as suggested by Weitzman (1999) there did not appear to be any one best program that might guide selection. Davidson and Gregorio (2011) note, however, that Dedoose is easy to learn, benefits from ongoing on-line software upgrades and patches, and is potentially adaptable for Cloud computing.

Capability	NVivo	Atlas.ti	Hyper-Research	Dedoose
Analysis function	Predefined & query	Predefined & query	Query	Predefined
Linking codes	Hierarchy	Complex network	Simple network	Hierarchy
Authority	Simple	Simple	None	Elaborate
Interleaved coding	File sharing	File sharing	File sharing	Server-based
Simultaneous coding	None	None	None	Synchronisation
Learning curve	Steep	Steep	Gentle	Medium

Table 6-3: A comparison of mainstream project data management software (Nielsen 2012).

Dedoose is also useful for its inherent mixed methods analysis capability, plus the application is a web-based data management tool, thereby offering cheaper, more powerful capabilities and less chance of performance degradation than a program downloaded onto a home or office computer. Dedoose projects can also be made available on the Web to authorised multiple users, which potentially facilitates easy repeatability and traceability of information analysis. Dedoose was chosen primarily for the research project's qualitative data management, and quantitative work was performed with statistical software package, SPSS. In retrospect the use of Dedoose program might have been useful during the literature review chapters, wherein a large quantity of journal articles and texts were manually searched, catalogued, indexed and then cross-referred towards the relevant topics.

6.9.2. Quantitative data analysis

Numerous statistical software packages are available for home or office machines, with some requiring online or cloud-based access, and these packages are either open-sourced, free or commercially marketed. Cavaliere (2015) notes that at least 50 statistical software packages are available for research users, and that the top

ten in this list have very little to differentiate one from another. However, within the literature, researchers are often seen to make use of programs R, SAS, Matlab, Statistica, Minitab, Statgraph and SPSS (Ertuğ & Girginer 2014; Bergtold, Pokharel & Featherstone 2015). For this research, SPSS (Statistical Package for the Social Sciences) was chosen due to its affordable price within an educational package for students, its ability to perform the required analyses and data outcomes, its popularity with fellow students, and the ready availability of user manuals on campus.

Selection of statistical data analysis techniques was limited by the small population of Australian port managers, which, for example precludes the use of factor analysis where typically, sample size needs to be closer to 100 (Urdan 2017). The use of inferential statistics was also constrained by the small potential number of participants. The primarily ordinal (non-parametric) nature of the quantitative question design and data characteristics effectively steered the analysis selection process (Pallant 2016).

The treatment and analysis of quantitative data were performed with the following techniques, according to how the questions were asked, the format of the gathered information, and the relationships to be explored (Pallant 2016):

a) the Mann–Whitney u test (a non-parametric equivalent of the independent t test);
b) the Chi-square test of independence – (to explore the relationship between two categorical variables);
c) the Spearman rho and phi coefficients (for measuring the direction and strength in corresponding relationships between variables);
d) Kendall's tau – *b* (while interpretations of Spearman's rho and Kendall's tau are similar, *b* enables a direct interpretation of the probabilities of observing the agreeable (concordant) and non-agreeable (discordant) pairs, but is less sensitive than Spearman's rho); and,
e) Kendall's Coefficient of Concordance – W (to determine the degree of agreement).

Both descriptive and inferential statistical techniques were employed in analysing and describing the data, and results were presented by means of tables and graphs.

6.9.3. Reliability and validity

Research reliability refers to repeatability, whereby research results remain consistent over time, and are seen to accurately represent the total population under study (Golafshani 2003). To optimise reliability the researcher must ensure the internal accuracy and reliability of test scores (Golafshani 2003). In this thesis, Cronbach's alpha coefficient was used to assess the internal consistency of the survey instrument scale used for measuring risk and resilience management capabilities and capacities (Vacha-Haase & Thompson 2011; Dunn, Baguley & Brunsden 2014). There was recognition that some questions contained fewer than ten items, and the data analysis was planned for a Cronbach level of greater than .5 (Gliem & Gliem 2003). Further efforts to increase internal reliability included clear item writing and expression within the survey to maximise variability in responses (Clark & Watson 1995).

Judgement is required, in when to use the 'Alpha if item deleted' facility available in the SPSS software, which might enable the researcher to gain a higher reliability figure (Pallant 2016). This facility to manipulate item reliability evaluation assumes that equal error variance exists across all items being examined. However, recognition was made that if an item with the smallest variance is deleted, it might carry less error than the remaining items, be more representative of the population value, and consequently make the instrument scale a more reliable measure of the data under examination (Dunn, Baguley & Brunsden 2014). Care was taken to enhance content validity, by ensuring so far as possible that the survey instrument was entirely relevant to the research problem under investigation and aligned with the factors discussed and identified within the literature review chapters.

6.10. Survey administration

Consideration was given to the quality of data to be collected by the web-based survey, and to the precision of inferences made about the studied population of port managers. An early component of the survey administration was to evaluate contributing factors to survey errors, and consideration of control measures to minimise error potential. Considerable time was expended in compiling a list of recent email addresses to minimise potential for undeliverable surveys.

6.10.1. Documentation

Participant recruitment primarily involved a proforma letter (Appendix A) sent as a custom email invitation attachment to the targeted managers. The managers' responses were to be tracked to see if they have taken the survey. As a preliminary step, high level sector promotional assistance towards the survey was sought from the ports' peak body group Ports Australia, in an endeavour to reduce the possibility of managers or their email systems rejecting the invitation to participate as spam, as sometimes occurs when email invitations are distributed (Koo & Skinner 2005). This assistance was requested by means of a formal letter once University of Tasmania Ethics Committee approval for the research was received (Appendix B). It was possible, but considered unlikely that promotional assistance from sector peer groups might lead to unexpected participation of respondents outside of the mail-out list, a phenomenon that Marcus *et al.* (2017) describe as a 'snowball' effect that potentially brings unwanted biases. Further, the introduction of any aspect of open-ended recruitment might reduce control over the makeup and size of the participant pool, which is why attempts were made to avoid the possibility of a snowball process. Plans were made to send an initial reminder to potential participants in two weeks from deploying the survey (Appendix A).

An online consent form accompanied the survey, and this was inserted into the online survey questionnaire. Participants could only perform the survey if they clicked the 'I agree' icon to acknowledge the informed consent conditions. Real names of respondents were collected, and these were matched with pseudonyms that will thereafter be the only form in which identities are referenced. Only the

researchers will ever see the linked names/pseudonymic codes and these were stored separately from the rest of the data. To further safeguard the conduct of the survey, the researcher and supervisors planned to meet fortnightly in the early stages of the research project, and following confirmation that the process is proceeding satisfactorily, to then revert these meetings to monthly events. Arrangements were also made that should an urgent problem occur that requires the attention of all researchers, then an immediate meeting would be arranged via a telephone linkup in the first instance. Arrangements were made for all raw data to be kept under lock and key, and for electronic documentation to be password protected where considered necessary.

6.10.2. Bias management and control measures

The Oxford Dictionary of English defines bias as a systematic distortion of a statistical result due to a factor not allowed for in its derivation (Simpson 2018). Some degree of bias is regarded as almost inevitable within a research project, and there is a possibility that bias might occur in the thesis preplanning and design stages, data collection and analysis, and when relating the findings and conclusions (Pannucci & Wilkins 2010). Bias can also arise, for example, when systematic error takes place in sampling or testing through selection of one outcome or answer above all others (Pannucci & Wilkins 2010; Creswell & Creswell 2017).

Potential arises within web-based surveys for sample frame and nonresponse bias (Fleming & Bowden 2009; de Vaus 2014). Sample frame bias occurs when a sample fails to represent the population that it is required to represent (de Vaus 2014). A control measure when defining the population is to establish an unbiased sampling frame from the population, however the sampling frame was made somewhat inflexible by the Australian port authorities general policy of only permitting designated spokespersons to respond to surveys (Gray 2017; Lewis 2017). These designated managers are senior executives who are authorised to speak from the corporate perspective, and include CEO's, Harbourmasters and heads of department within their port organisations (Lewis 2017). These spokespersons are likely to provide representative information concerning their

port's risk management and resilience processes because they are influential decision-makers in these areas. Specific bias potential and some control measures that are observed within this thesis are shown in Table 6-4.

Bias categories	Bias controls
Selection bias: May result in the subjects in the sample being unrepresentative of the population of interest – it occurs when the groups to be compared are different.	Take rigorous care to ensure that participants are chosen from the same general population
Measurement biases: Issues that are related to how the outcome of interest was measured. Can arise from multiple sources.	Careful wording of the questions and unobtrusive redundancies that permit the researcher to determine whether internal inconsistencies exist.
Respondent bias (Acquiescence and Habituation): Respondents either tend to choose answer that represent their organisation favourably, or tick 'down the line' using the same answers to finish the survey quickly.	Design questions that focus on garnering the respondent's true point of view. Maintain respondent interest with engaging survey design. Vary question wording, types of questions, and order of answers within questions.
Confirmation bias: Researcher frames survey questions in such a way to confirm the researcher's hypothesis or concepts.	Continually revaluate impressions of respondents and challenge pre-existing assumptions and hypotheses
Question order bias: leading questions, and where the answer to one question suggest how the next question might be answered.	Careful wording and arrangement of questions, for example a general question on a subject before a specific question.
Ignorance bias: Researcher not knowing which statistical test to apply. Also applies to respondents knowing little about the subject under survey.	Conduct tests to assess the suitability of the data for the relevant process. Taking care in selecting potential participants in the survey.
Non-response bias: Respondent failure to answer one or more questions, or the entire survey.	Reminders, industry support, and survey design where progress to the next group of questions requires answers to the previous questions.

Table 6-4: Potential web-based survey biases and control measures (Adapted from Lavrakas 2008, and Biffignandi & Bethlehem, 2012).

Pretesting the survey played a prominent role in minimising survey errors and in reducing bias. Researcher bias was minimised by observing ethical guidelines which are now discussed.

6.10.3. Compliance with ethical guidelines

When designing the questionnaire, care was taken to ensure that participants were not exposed to unfair or unethical demands, and that the researcher observed ethical guidelines as approved by the University of Tasmania Ethics Committee. Ethical considerations included privacy, confidentiality, anonymity, research integrity and quality, and in the web-based survey context, maintaining the online confidentiality of respondents' identities within the survey instrument,

and in avoiding potential situations where research quotes from responses to open-ended questions might be searchable with online search engines (Schutt 2012).

To comply with the ethical dictum not to cause harm, the research interview and surveys were firstly submitted to supervisors for approval, and then tried out in the form of pilot studies involving other students. Informed consent as required was obtained only after the researcher observed the ethical obligations for maintaining respect in research communications, and to fully advise interview and survey participants of the project's nature, their right to refuse participation, the researcher's responsibilities, and any risks or benefits that the participant might expect from the study (Polit & Beck 2004). As previously discussed, an online consent form accompanied the survey, and respondents were unable to access the survey without clicking on the 'consent' icon.

The first section of the survey questionnaire established the demographic segments within the population, whereby causal factors might relate to differences in responses and understandings. The second section sought information on disruption types and causalities, and the third section investigated how and with what means managers responded to and managed disruptions over the past five years. The fourth section explored port management capabilities for maintaining operational services following a high consequences disruption. Port organisational resilience capabilities, leadership and governance, inclusive of stakeholder collaboration are then investigated to assess how far resilience might be embedded within Australian ports, what impediments might stand in the way of increasing resilience levels, and the potential for operationalising port resilience.

A minimal risk application was completed in consultation with supervisors and forwarded to the University of Tasmania Ethics Committee, with associated documentation inclusive of the draft survey questionnaire and accompanying emails and letters, which are attached to this study as Appendices A-D, and the subsequent Ethics Committee approval is attached as Appendix B.

6.11. Summary

Chapter 6 provided an explanation of decision-making processes and rationale employed for the research methods, data collection and analysis techniques of this study. A web-based survey of Australian port senior executives was designed from a mixed methods approach to address the research gaps and questions identified from the literature review (Chapters 2-5). The quantitative findings were to be explored in greater depth and triangulated where possible with qualitative analysis. Data analysis was planned around the use of SPSS software for quantitative data, and the Dedoose online software was selected for qualitative data analysis. Results of these analyses will be presented in Chapter 7 (risk management findings) and Chapter 8 (resilience findings). Two data analysis chapters were planned because the analysis process in this case is lengthy and shorter chapters make the reader's task easier. Further, assigning individual chapters to the risk and resilience data sets was useful in avoiding the possibility of concept confusion.

Chapter 7: Data analysis and interpretation of findings

7.1. Introduction

Chapter 7 investigates and interprets the risk management data gathered from the exploratory survey process, and where judged beneficial to the research objectives, links these findings with those gathered from secondary sources. This data investigation involves analyses of both quantitative and qualitative data, with the findings from the initial quantitative phases both informing and guiding the qualitative phases (Onwuegbuzie & Combs 2011). The data analysis is geared towards addressing the primary research objective of understanding how Australian ports manage the risks and outcomes of regional disruptions. The data also provides interpretations of port disruption categories, how managers have coped with disruptions, port risk management effectiveness, predictions of future risks and management preparations for these future risks.

7.2. Chapter processes

The first three sections of this chapter encapsulate the entire data analysis process in the form of a general overview. Chapter 7 then goes on to discuss the port risk environment and continues with the analysis of risk management responses for the remainder of the chapter. Chapters 7 and 8 employ elements of both quantitative and qualitative analysis, and where quantitative analysis might be additionally informed from qualitative findings, a mixed methods analysis process. Some qualitative information is quantified when processing freeform answers that amplified or explained primarily quantitative responses. Data analysis in each area of investigation sequentially follows the order of survey questions. As detailed within Chapter 6 research methodology, the coding, sorting, entering into the computer and subsequent processing employed a combination of Excel, SPSS and Dedoose software.

7.3. Response rate

One hundred and thirty-one invitations to participate in the survey were sent to Australian port managers, with 50 surveys returned. The rate of return reflects the relatively small pool of port managers employed at senior levels across twenty-

seven port authority and government entities tasked with responsibilities for managing Australian ports. While conducting the survey, advice was received from a Ports Australia Board member (Lewis 2017) that Australian port authorities typically authorise only one or two of the most senior executives to participate in surveys that sought information on a corporate view, so that the potential pool of respondents was re-assessed to be 54. A power calculation established that with a population of 54, a confidence level of 95% and a margin for error (confidence interval) of +/- 5, then 47 respondents are required (Denscombe 2014). Thirty-seven respondents fully completed the survey, which from an aspirational confidence level of 95% resulted in a +/- 9% survey margin of error. Statistically, this indicates that if 50% of the sample provides an answer then of the entire population between 41% (50 - 9) and 59% (50 + 9) might provide a similar answer. However, 37 respondents do not provide a sufficiently large sample to be statistically significant, and the research cannot demonstrate internal significance/reliability from such a small sample.

Meterko *et al.* (2015) study response rates for surveys involving senior level executives and conclude that survey results 'should be considered on their merits even if based on relatively "low" response rates'. Researcher confidence in the sample size and wider applicability of the research findings is also enhanced by the relative homogeneity of the respondents in terms of their management functions. Respondents are senior port executives vested by their Boards and State governments with similar authoritative decision-making roles, duties responsibilities, and compliance functions. Generally, respondent demographics show that the respondents have more than three years' experience in their present positions.

Denscombe (2014) argues that studies of small organisations will likely result in small sample sizes, and that so long as the sample is larger than 30, and that statistical limitations are acknowledged and considered, then the study findings might remain both informative and valid. In this research the respondents are authorised spokespersons and lead decision-makers for their organisations and capable of providing accurate and high-quality information about organisational

risk management strategies, behaviour, processes and intentions. Further, the survey questions probe deeply into multiple aspects of port risk management and resilience, and according to Denscombe (2014) investigating in depth serves to further study integrity. For these reasons the absence of statistical significance resulting from sample quantity is somewhat masked by sample quality, and the argument that respondent homogeneity tends to characterise the respondents as representative of the Australian senior port manager population.

Of the 50 responses, 37 were useable and seven were partly useable, but in calculating response rate only the 37 completed responses were considered valid overall. With a senior management pool of 54 accessible to this survey across 27 port management agencies, then a response rate of 37 effective surveys is calculated to be 68.5%, which is higher than a typical level of return from senior executives for web-based surveys (Simsek & Veiga 2001; Rogelberg & Stanton 2007; Stephenson 2010a).

A global decline in survey response rates is noted by Rindfuss *et al*. (2015) and particularly so for telephone surveys (one reason why this research opted for a web-based survey). For whatever reasons, senior executives appear least likely within an organisational context to respond to internet surveys, with some studies reporting senior executive response rates as low as 7% (Simsek & Vega 2001). Conjectural reasons for relatively small response numbers might include practitioners limited organisational resilience understandings (Stephenson 2010a; White & O'Hare 2014). Further, a possibility exists that some port managers are unfamiliar with organisational resilience and resultantly uncomfortable with providing their opinions. Response rates fell from the initial 51 (94%) who began the survey, and only 37 (68.5%) fully completed the questionnaire. Thirteen (24%) filled out the questionnaire's initial demographics section but left further questions blank.

Three waves of emailed letter reminders were sent (Meterko *et al.* 2015), and the researcher avoided antagonising managers with further reminders. Non-response error had been minimised so far as possible, and the number of non-responses and partial responses suggests that important information regarding port

managers with a low level of risk management and resilience understanding was not gathered. This non-response bias could mean that data findings are biased towards the more resilience-conversant port organisations. Whereas the recorded response rate minimises statistical generalisability of research findings to the wider Australian port management population, the data quality relating to the high level of port executives who participated in this research lends importance to the information obtained.

Rindfuss *et al.* (2015) suggest that low response rates do not invariably indicate biased results or necessarily equate to low data quality, particularly if relationships between the variables are examined within a multivariate rather than univariate distribution model. Multivariate data analysis enables the simultaneous investigation of multiple variables to better understand their relationships, generally in the form of either exploratory data analysis or regression analysis (Anderson 2003; Swarbrick 2012; Pallant 2016) or where required, as numerical taxonomy - the sorting and categorising of cases into like kinds (Jupp 2006). Information gathered from survey respondents was provided in forms suited to both parametric and non-parametric analysis, with the high number of Likert type questions emphasising the use of non-parametric correlation coefficient measurement - primarily Spearman's rank order correlation, and Kendall's tau-*b* measure of probability.

7.4. Survey participant demographics

Descriptive statistics were used to analyse demographic factors. The survey questionnaire was distributed to potential participants whose email addresses were publicly available, from a thorough online search of port-related data bases. Fully completed surveys were returned by 37 respondents (5 CEO's, 2 Managing Directors, 8 Harbourmasters and 22 senior executives = 75% of the 49 in total responses). Survey returns are shown in Figure 7-1, and an explanation was considered towards the 25% partial completion rate for returned surveys, where respondents clicked upon the 'completed' icon despite not fully filling out the form. Within this context, Bosnjak and Tuten (2001) explore the web-based survey partial completion phenomena and suggest that reasons for partial completion

might include either lack of respondent motivation, lack of opportunity or cognisant ability, and/or being uncomfortable in answering certain questions.

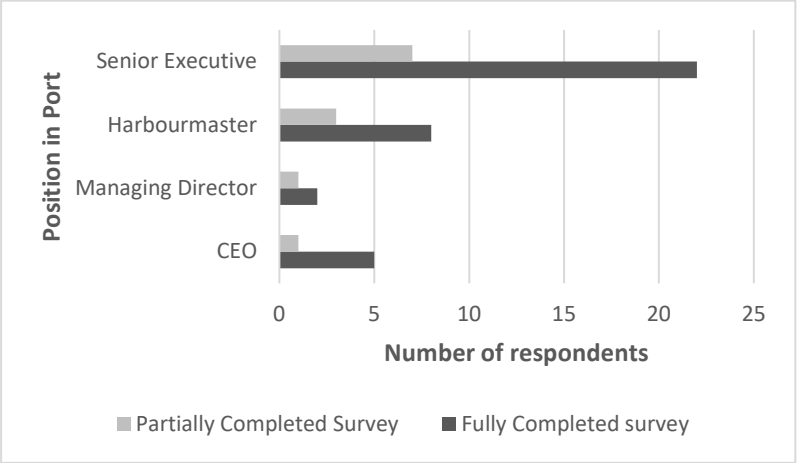


Figure 7-1: Response rate demographics (Author).

Within this survey, almost all partial completions involved respondents filling out the initial and compulsory demographics section, and then reading through the online survey form until logging out. Bosnjak and Tuten (2001) describe this participant behaviour as *Item non-responding drop-outs* whereby a participant views some or all questions but only answers some and then terminates the survey. Bosnjak and Tuten (2001) suggest that this is quite typical survey behaviour. Intuitively, further drop-out rationale in this research might occur from participant sensitivities in discussing port vulnerabilities and emergency management capabilities in a post-9/11 threat environment.

Demographics included tenure within the management roles, as shown in Figure 7-2. Eight senior managers were female (16%). One executive had served for less than one year (2.7%); five for less than three years (13.5%); ten had served for between three and five years (27%); and, twenty-one had served in their roles for more than five years (56.8%). These demographics indicate that senior Australian port management positions are predominated by male executives with more than three years' experience in their roles.

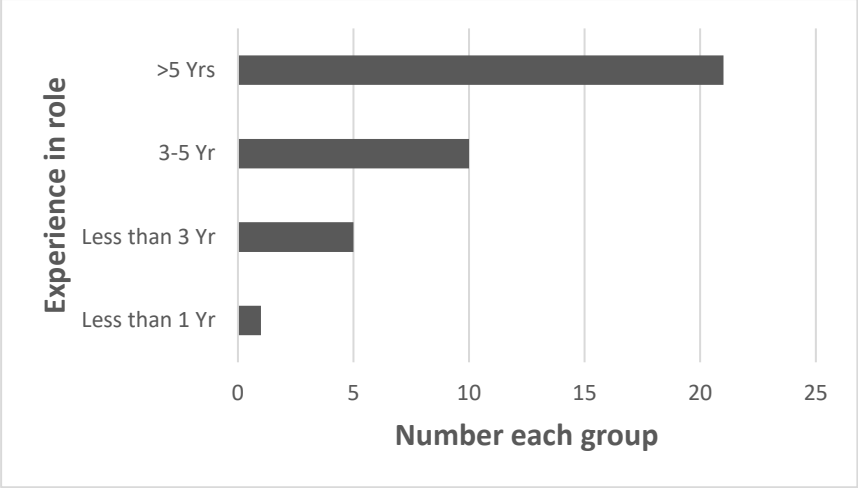


Figure 7-2: Australian senior port managers experience in roles (Author).

Four senior managers with nil risk management qualifications had between three and five years in their roles, and four exceeded five years seniority. Eight managers, including three CEO's, experienced all risk management training in-house; one had less than three years' experience in the job, one between three and five years, and six exceeded five years seniority. The remaining managers held multiple risk management qualifications as shown in Table 7-1.

Qualification	**CEO/General Managers (7)**	**Harbourmasters (8)**	**Senior executives (22)**
Nil held	2	0	3
Course module within a professional degree	2	2	10
Certificate level	0	2	4
Diploma level	0	0	2
Professional development short course	0	5	10
Commercial course qualification	0	0	4
In-house training	3	4	11

Table 7-1: Survey respondents risk management qualifications (Author).

Lansdale (2012) describes how the Harbourmaster or port operations manager is assigned to manage port operational activities and, in many cases, to also command an emergency operation centre in the event of a port disruption. In the event of a disruption, a senior executive is appointed to speak on behalf of the organisation and handle media enquiries. This port emergency operations centre media spokesperson is likely to be the CEO or equivalent person in charge (Lewis 2017). The literature review findings suggest that competency in both command

and control roles in business-as-usual circumstances, and in emergency management roles requires risk management knowledge and leadership skills (Lansdale 2012; Burns 2015) and a lack of formal risk management qualifications or training might be a competency handicap.

7.5. The port risk environment

Eleven hazards with potential to cause port disruptions were selected for testing as shown in Figure 7-3. These hazards were selected from an extensive literature review and expanded to incorporate suggestions made during the survey testing phase. Climate change might more accurately be termed a threat if considered to be an actualised hazard resulting in increasingly severe weather events, higher daily temperatures and expanded tropical disease vectors (Kelly-Hope, Purdie & Kay 2004; Maunsell 2008; Russel *et al.* 2009; Ng *et al.* 2013a; Naish *et a*l. 2014; WEF 2018).

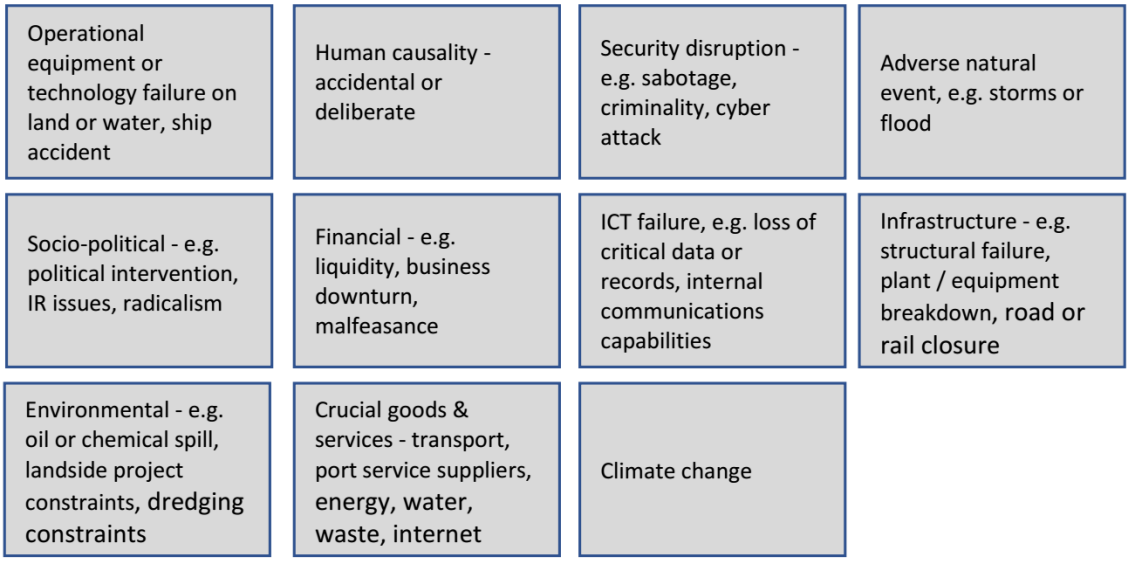


Figure 7-3: Port disruption categories for testing (Author).

7.5.1. Number of disruptions

In response to how many disruptions respondents had experienced during 1) the past twelve months, and, 2) the past 1-5 years, thirty-four answered this question. Where managers had served less than five years or more in their roles (see Table 7-1), their corporate memory of recent disruptions would have been expanded during annual risk management evaluation and brainstorming sessions (Srikanth

& Venkataraman 2013; Bichou, Bell & Evans 2014; Burns 2015). The respondents' collective answers to this question are shown in Figure 7-4.

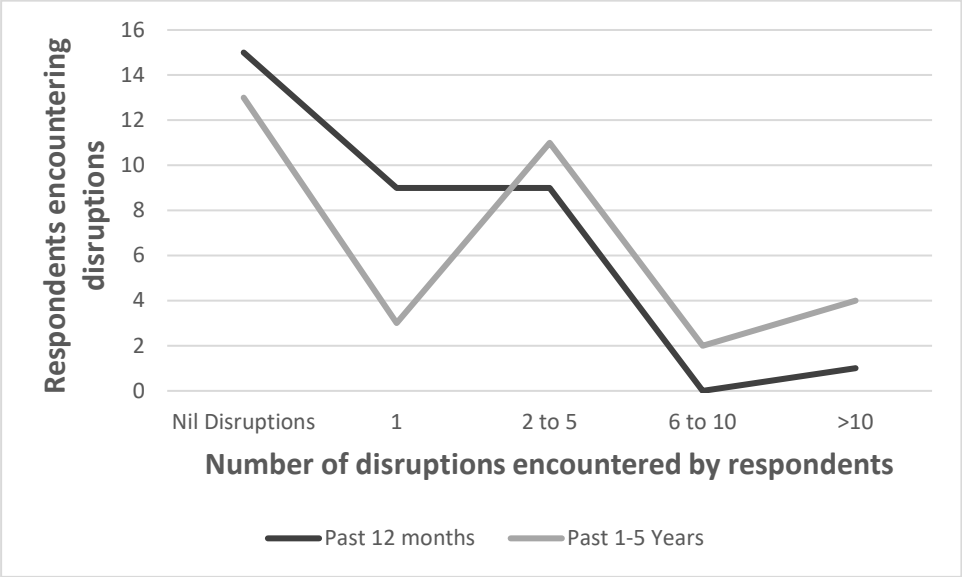


Figure 7-4: Disruption experiences over short and medium time frames (Author).

Figure 7-4 shows that shows that 19 respondents experienced port disruptions during the past twelve months and of these, nine (26%) experienced single disruptions, and ten (29%) experienced multiple disruptions (nine encountered 2-5 disruptions that year, and one experienced more than 10). During the four years prior to these twelve-month figures, 20 respondents (64%) experienced port disruptions, and 20 respondents (59%) experienced multiple disruptions over the four years. In total, thirteen managers experienced nil disruptions during the five-year period (35%).

Eleven respondents experienced 2-5 disruptions, two experienced 6-10 disruptions and four respondents experienced more than ten throughout that period. These findings indicate that Australian port managers experienced a higher proportion of nil or single disruptions during the past year than during the previous four years period. However, cognisance is made that the annual numbers of disruption occurrence are influenced by short and long-term cyclical patterns and occurrences which might serve to average the 'nil disruption' level lower over time (Grinin, Korotayev & Tausch 2016). Examples of these cycles include the onset of extreme El Niño events (Nott 2018), financial cycles varying from benign to crisis

level states (Rey 2015), and climatic variabilities resulting in droughts, bushfires or floods (Kiem *et al.* 2016; Ummenhofer & Meehl 2017).

7.5.2. Predicted risks

Risks previously experienced by port managers and those predicted for the coming years are shown in Figure 7-5, which is a composite of respondent experiences with disruptions of the past five years, and their expectations of what might challenge them during the next five years. Adverse natural events are the highest future risk (12 predictions), followed by financial constraints (11 predictions) and then socio-political risk (9 predictions). Increasingly severe weather patterns were a primary concern within respondent free-form responses, possibly influenced by increasingly severe storms and floods affecting both Australian and global ports (Elsner, Kossin & Jagger 2008; McBride 2012; Wakeman 2013; Tracey 2011).

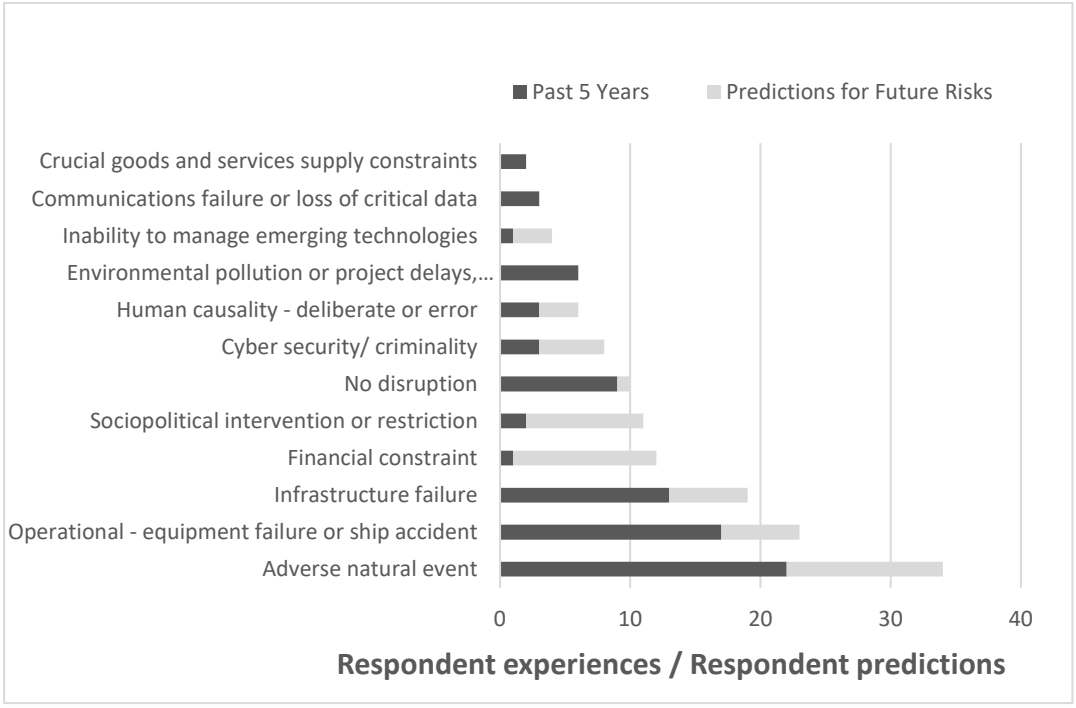


Figure 7-5: Comparison of port disruption typologies – composite of past vs. predicted (Author).

Free-form responses reflect a concern for political interventions that associate problems involving infrastructure failure, socio-political issues, and financial constraints – both analysed later in this chapter. Financial concerns relate to port inability to maintain or replace infrastructure and plant at a time when State and territory governments (the port owners) experience public sector financial deficits (ABS 2017). Ports pay annual dividends to their State government, usually 65%of

net profits (Evans 2015) but with the present levels of State government financial stress, ports are required to pay higher dividends to their governments. For example, the Western Australian State Budget (2017) increases government business agency dividend rates, whereby multiple port authorities contribute some 90% of their net profits. Uncertainty also stems from port management knowledge of State government considerations towards asset sales in reducing State deficits and funding other infrastructure, inclusive of marketing ports and port property. This concern is consistent with findings from Chen, Pateman and Sakalayen (2017).

Twenty-eight respondents expressed in free-form answers why they identify their most likely port risks for the next five years, and their insights contribute to the primary research question (how Australian port managers manage the risks of high consequence disruptions). From these qualitative rationales an unexpected, different pattern and order of disruption emerges to that of the closed-ended data. Patton (2015) describes providing quantitative and qualitative aspects of the one question as opportunities for comparative analysis between the two techniques, and for increased understanding by focussing on areas of convergence. In this case, researcher understanding is clouded by areas of divergence between the quantitative and qualitative data. However, the two types of analyses produce similar lists of future risks, but at differing levels of likelihood.

7.5.3. Associations between past and predicted disruption occurrences

Past disruption types were compared in Table 7-2 with respondents' expectations for port disruptions during the coming five years. This shows that respondents expect fewer port disruptions to occur in the near-term future. However, disruptions of human causality, cyber-threats and socio-political hazards opposed this trend. Despite 35% (13 respondents) having experienced nil disruptions during the past five years, only one respondent expected circumstances of nil disruptions for the coming five years. For the remainder of disruption categories listed, managers expected fewer occurrences in the future and nil recurrence of communications failure, environmental pollution and failure of crucial goods and services supply.

Disruption Typologies (each column shows number of respondent nominations for each typology)	**Past 5 Years (actual)**	**Predictions for Next 5 Years**
No disruption	10	1
Operational - equipment failure or ship accident	15	6
Human causality - deliberate or error	3	3
Cyber security/ criminality	3	5
Adverse natural event	19	12
Socio-political intervention or restriction	1	9
Financial constraint	1	11
Communications failure or loss of critical data	2	0
Infrastructure failure	11	6
Environmental pollution or project delays, dredging constraints	5	0
Crucial goods and services supply constraints	2	0

Table 7-2: Port disruption contingency table – comparison past five years (actual) with port predictions for next five years (Author).

Respondents' expectations of fewer disruptions in the future from previously experienced causalities appear to be inconsistent with the literature and intuitively, somewhat illogical (Guha-Sapir, Hoyois & Below 2014; Blaikie *et al.* 2014; Arouri, Nguyen Youssef 2015; WEF 2018). Further, respondents overlook altogether the potential of future risks involving port communications, data management security and cloud system failure. Also overlooked is future potential for adverse environmental events, and the failure of crucial goods and services supply. To test whether inconsistencies exit between examples of past and future disruptions (categorical variables) a cross-tabulation test was performed.

A limitation of cross-tabulation testing of Table 7-2 disruptions is that only three categories of disruption provide reported nominal values of five and over (shaded) and these involve operational, adverse natural event and infrastructure failure. Cyber-threat (also shaded) was added to this testing list despite its low levels of occurrence, because technology is increasingly important to critical infrastructure business continuity, inclusive of port operations (Meyer-Larsen & Müller 2018; Paté-Cornell *et al.* 2018). Further, the literature indicates that cyber-threat is a source of risk to port operations (Roth & Nakashima 2017; Tucci 2017).

A chi-square (**χ^2**) test for independence compared four of the 37 respondents' reported port disruptions, with the number of these disruption categories that they expected during the near-term future. The purpose of the test was to establish if evidence of a relationship exists between the observed numbers of disruptions and prediction numbers. The null hypothesis is that there is no significant relationship between past and future categories of disruption. Testing results are shown in Table 7-3, using one degree of freedom, 2X 2 tests of independence, and Phi (McDonald 2014). Yates correction was not used as this gives a high p-value for tests of independence. To make increased sense of data findings, McDonald (2014) suggests pooling variables with multiple categories containing few numbers, as is the case for seven of the port disruption hazards. This technique was added to the test, by pooling hazards of human causality, socio-political, financial, environmental, crucial goods and services failure under the heading of 'other'. The null hypothesis (H_o) is that no relationship exists between past observances of the hazard categories, and predicted occurrences – that is, the evidence indicates that the two categorical variables are not related (Pallant 2016)

Causality	**χ^2**	**p**	**Fishers Exact (2t)**	**Fishers Exact (1t)**	**Phi & approx. significance**	**Level of Association (a)**
Operational failure	5.385	.020	.038	.190	.270; .020	Weak
Cyber-threat	.561	.454	.711	.355	-.087; .454	Weak
Adverse natural event	2.72	.099	.157	.078	.192; .099	Strong
Infrastructure failure	1.909	.167	.269	.134	.161; .167	Nil
Other	6.618	.010	.019	.009	-.299; .010	Nil

Table 7-3: Chi-square test for independence between past disruptions and predictions (Author).

Except for adverse natural event hazards, there is minimal relationship between the number of observed disruptions within specific categories and the predicted likelihood of similar disruptions occurring in the future. Further, the SPSS 'expected count' figure for predicted hazard occurrences generally shows more than respondent predictions. An exception occurs with pooled hazards under the heading of 'other' where respondent concerns regarding perceptions of increasing likelihood for socio-political and financial constraints weights the outcome

towards future risks. In the case of these 'other' hazards, past occurrences of disruption were 27% less than what might be expected, whereas predicted occurrences for the near-term future were 21% higher than what might be expected. The disparity between the types and numbers of disruption experienced in the past, and general expectations for fewer of these disruptions in the short-term future appears to be illogical, and perhaps worthy of further research.

Whereas port managers' self-reports of disruption causality in the past are likely to be verifiable, their predictions for the future are qualitative and subjective, and outcomes can only be verified at some time in the future. What can be shown is that predictions of future disruption occurrences are generally less than what might be expected based upon the numbers of previous events. The disparity might be partially explained by the concept that port managers are likely to conceptualise multiple, subjective, sometimes contradictory but equally plausible perspectives of future risk (Stirling 2007). The impact of an incorrect estimate of future risks and port vulnerabilities assumes importance when port managers conduct their operational risk assessments. An inadequate risk assessment process potentially results in less priority given to risks that deserve higher levels of treatment, or alternatively, of higher priority being afforded to less probable risks (Suter 2016). These possibilities are examined more closely in the next section.

7.6. Port disruption management

The process of assessing respondents' self-reported performance capabilities against high consequence disruptions requires an understanding of risk management behaviour with past events, and how well these were managed, coupled with an estimation of whether similar risks might reoccur (Haimes 2016). For this reason, the survey questioned past emergency management capabilities and capacities, and sought forward-looking information related to port potential in treating and managing an uncertain risk environment. Managers were presented with a total of ten port-related hazard categories that were identified from the literature (including Jüttner, Peck & Christopher 2003; Ronza *et al*. 2003; Darbra & Casal 2004; Handfield 2007; Alderton 2013; Mazaheri *et al*. 2014; Burns

2015; Bichou 2018). Port management self-reports on their abilities to cope with these disruptions were analysed for relationships and commonalities and evaluated for factors indicative of their risk management capabilities and capacities. Respondents (n = 39) reported coping capabilities under the headings of either 'coped, barely coped, unable to cope, somewhat unable to cope (external assistance required), unsure, or not applicable'. Their responses were coded and tested for internal consistency and reliability, with Cronbach alpha of .7330, n = 10 items.

The findings suggest that risk management analysis is not necessarily a cut and dried process of ranking the greatest number of respondents affected by the greatest number of disruptions. Some disruption categories might be managed relatively quickly and effectively, whereas managers might struggle to cope with others, or even need to call upon external assistance. A further limitation of this assessment is that hazard impacts and consequences might vary in severity and closeness, so that a minor category one cyclone, for example, might approach the port closer than a more severe weather event which is managed with less port downtime.

Australian port abilities to cope with the hazards under consideration were assessed from self-reported disruption management information (Q10 of the survey questionnaire). In some instances, port managers held no recent experience with one or other categories of disruption and entered a 'not applicable' response. These not applicable reports were removed from calculations to leave a pool of managers who coped, those who barely coped, those who required external assistance to cope, and those who reported being unsure of their abilities to cope with various categories of disruption. Percentages were calculated for the pool of remaining participants, with the total for each category of disruption response at Figures 7-6 and 7-7 rounded up to 100%.

Port disruptions were defined within the survey questionnaire as unexpected or unforeseen events that result in major impairment to a port's operations for one day or longer. This time consideration served to filter a multitude of minor impairments to port operations, for example increasingly common experiences

with short-term technology or equipment failures (Burns 2015). Only one respondent reported 'unable to cope' with a past disruption, and this related to third-party socio-political constraints against dredging, which was a matter possibly beyond the port's capacity to redress.

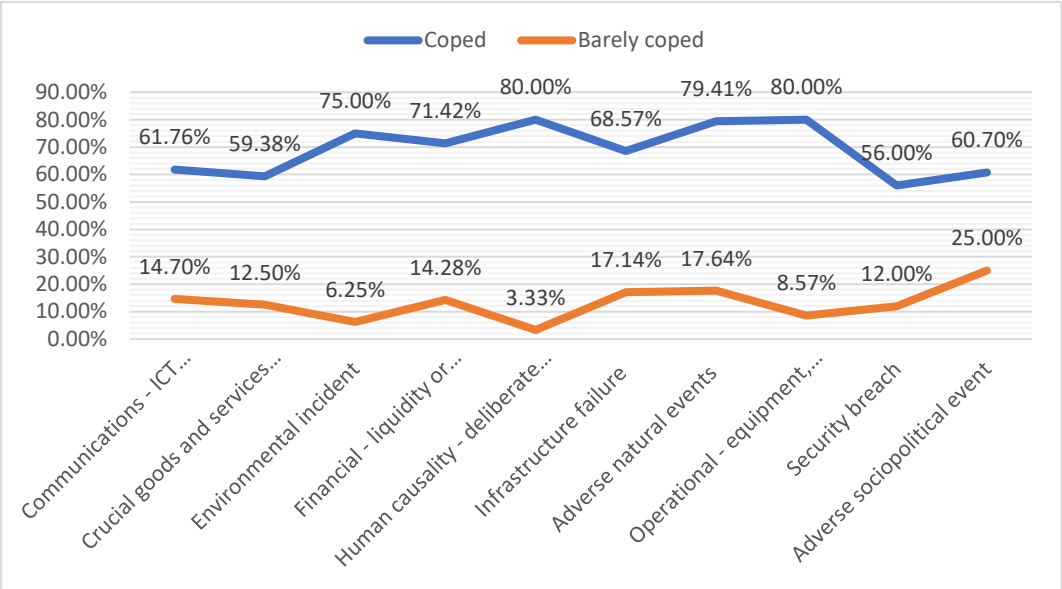


Figure 7-6: Respondent abilities to manage and recover from disruption categories (Author).

Respondent abilities to manage and recover from disruptions vary in effectiveness according to disruption categories, as shown in Figure 7-7. Respondents who coped with disruptions are grouped into two levels – those who self-reported effective responses, and those who struggled to manage and recover, albeit successfully. Levels of effective response for those who managed effectively varied widely between 56-80% of respondent numbers, with lowest levels of effectiveness recorded against security breaches and the failure of crucial goods and service supply. The highest percentages of effective responses were recorded against hazards derived from human causality, adverse natural events, operational plant and equipment failure, and ship incident. For respondents who experienced difficulties in coping, most challenging hazards were noted as infrastructure failure, adverse natural events, and adverse socio-political events. However, the pattern graphed at previous Figure 7-6 shows that the two levels of coping abilities are associated, that is where the percentage of effective management is highest, the percentage of managers with coping difficulties reduces.

Figure 7-7 reflects self-reports of risk management limitations, where port managers either cannot manage a hazard unaided, or are doubtful of their coping abilities against specific disruptions. These reports provide indicators of both risk management capabilities and vulnerabilities to risk. Respondents involved in these reports need to engage in remedial action against the possibility of similar hazard categories reoccurring, and in improving relevant risk treatment capabilities (Leveson 2015). The three highest levels of hard to treat threat are the failure of crucial goods and service supply, adverse natural events, and security breaches.

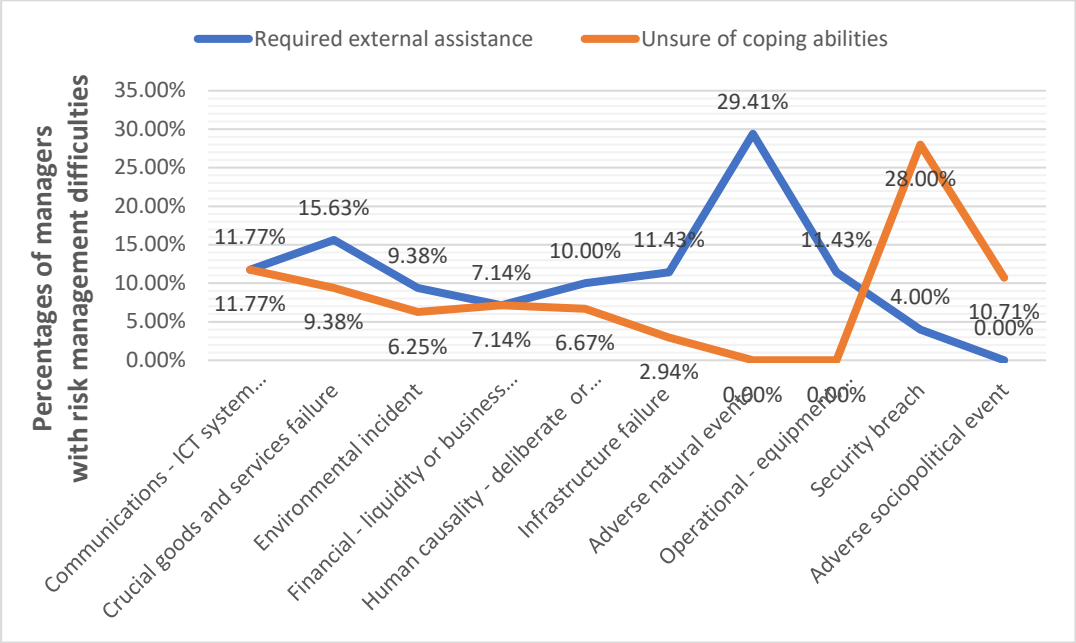


Figure 7 7: Respondent experiences with difficult port risk problems (Author).

Few comparable benchmarks were found with which to compare these self-reported levels of risk management competencies. Studies on US ports' disaster planning and recovery (GAO 2007; Trepte & Rice 2014) have findings consistent with this research, in establishing that some US port authorities have difficulties in effectively coping with disruptions. Trepte and Rice (2014) note that these US port managers struggle to manage damage to critical infrastructure; in maintaining critical goods and services supplies, communicating with external stakeholders, port personnel and critical goods and services suppliers; and with engaging in interagency coordination and collaboration. These factors are also explored within this thesis.

A variable pattern of Australian port effectiveness against individual categories of disruption is also indicated in Figure 7-7, where managers appear to fare best when disruptions involve physical manifestations of consequences. Disruptions related to more intangible or covert causalities (for example cyber-threat) appear to be more difficult to manage, and respondent effectiveness in treating intangible risks is markedly less than for those of more tangible causality. The findings indicate four levels of port risk management outcomes, where port managers:

a) respond, manage and recover from disruptions;
b) respond, manage and recover from disruptions, but with difficulties;
c) respond, manage and recover from disruptions with external assistance; or,
d) are unsure whether they can respond, manage and recover from these categories of disruption.

These findings suggest that gaps exist in Australian port abilities to cope with high consequence disruptions, and that where these gaps exist, risk and security management improvements would be beneficial.

7.7. Insurance and insurability

Collier (2008) questions when the growth and increasingly adverse consequences of catastrophic risks (for example terrorism, natural adverse disasters and technological failures) might compel insurers to reconsider their levels of client coverage in some risk sectors. An adverse endpoint of such a review might be cessation of coverage (uninsurability), and reduced use of insurance for risk mitigation (Collier 2008). Insurability is a relevant consideration for port managers challenged by new and emerging risks of the 21st Century. Port authorities/corporations are, in general terms, insured by their State governments. For example, Western Australia's RiskCover organisation insures against certain port risks, but places limitations and restrictions on the cover

provided[2] to ports because the government categorises port authorities as 'non-inner budget sector agencies'. Q9 explores whether port managers employ insurance as a means of risk transfer and examines the roles of insurance in port disruption recoveries across eight categories of operational risk. The academic literature is largely silent on the use of insurance within Australian port risk management and resilience, however the Australian Critical Infrastructure Resilience Strategy (AG 2015, p. 13) appears to argue that insurance is not an acceptable answer to risk, and that more needs to be done in other areas:

> Other organisations are able to take out insurance or put in place other 'hedging' arrangements to manage risk…(and) make a decision to discontinue normal operations until the threat dissipated, or things returned to normal. (For) critical infrastructure organisations, this approach is not appropriate and the Government has a role to assist critical infrastructure organisations enhance their ability to manage unforeseen or unexpected hazards.

This suggests that infrastructure operators (inclusive of ports) should concentrate on strengthening their resilience capabilities to remain operating in disruptive conditions, rather than look to insurance as either a risk transfer opportunity or a source of financial assistance in disruption recovery (AG 2015). Additionally, port managers are reminded by Clark and Hakim (2017) that insurance might cover certain critical infrastructure risks (for only certain aspects of risk), but will not cover intangible losses, for example losing port customers or reduced reputation or goodwill. O'Hare, White and Connelly (2016) suggest that reliance upon insurance is counterproductive because this reliance engenders a mindset that more readily accepts risky behaviour and resists change after crises. They argue that reliance upon insurance and is more attuned to an organisational return to the status-quo rather than adaptive reconfiguration of risk management

[2] See web site: https://www.icwa.wa.gov.au/riskcover/what-is-covered

behaviour. However, with ports' increasing exposure to multiple hazards (Lam & Lassa 2017), then insurance appears to be important in financing a port recovery from disruption.

The research assesses port managers' opinions on insurance cover as a partial means of mitigating or transferring a level of risk to another party. Port managers express both a high level of uncertainty and a lack of knowledge regarding insurability of a range of disruption risk drawn from the literature review. This mindset is consistent with other studies, which find that respondents experience ambiguity and uncertainty concerning organisational disruption insurance (Brown, Seville & Vargo 2013; Verdon-Kidd, Kiem & Willgoose 2016). The global Business Continuity Institute (Alcantara, Riglietti & Aguada 2017) establishes that while 65% of its surveyed supply chain members incurred at least one disruption to their operations during 2017, most of these disruptions were not insured.

Q9 comprises two exploratory components – reliance upon insurance in lieu of employing mitigation measures, and port managers' opinions about the extent and likelihood of insurance assistance for disruption recovery. In considering whether ports might rely upon insurance as a substitute for in-house mitigation measures for managing disruption risks, only 15% gave credence to this possibility (n = 34). Figure 7-8 shows respondent opinions on the reliability of insurance in covering multiple aspects of risks, suggestive that overall, few port managers are entirely confident of insurance as a reliable addition to their risk management tool chest.

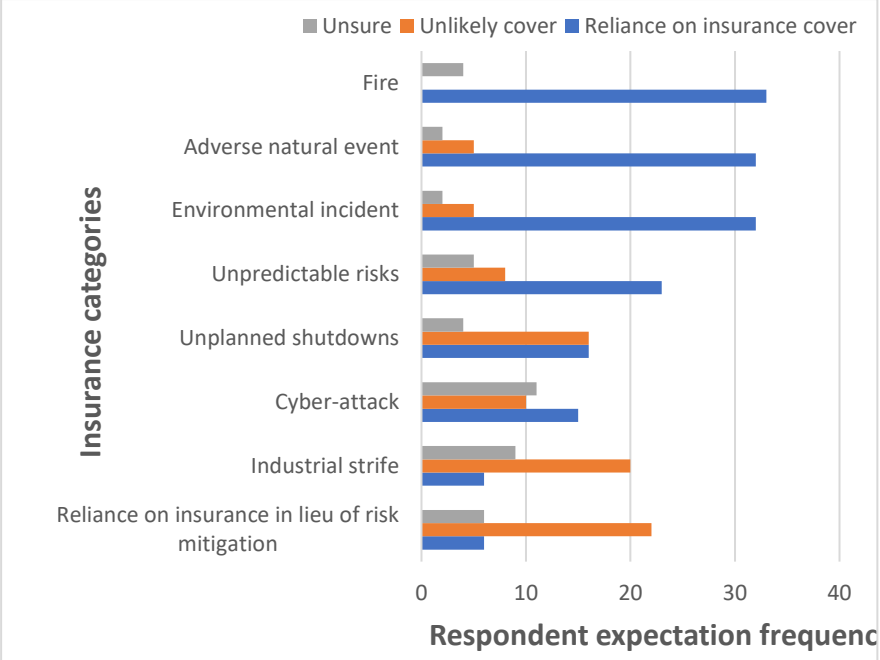


Figure 7-8: Port expectations on insurance coverage likelihood (Author).

The best-case scenarios are that half the respondents expect insurance to cover them for the consequences of severe weather events and fire. The least likely disruption types to be covered by insurance are cyber-attack, unplanned shutdowns, and industrial strife - with a lowest level expectation of 4.9% for unplanned shutdowns.

7.7.1. Insurance against individual disruption categories

Port dependencies upon ICT technologies for their operations, systems, equipment and records create in-depth vulnerabilities to cyber-threats and malware (DiRenzo, Goward & Roberts 2015; Newberry 2015). Increased exposure to these risk categories is negatively associated with dependability of insurance cover, with only seven of thirty-six respondents expressing confidence that insurance will cover unexpected/unforeseen and cyber risks. Managers' expectations for insurance against cyber-threat might improve in the short term, once insurance companies begin to provide specific policies that cover the consequences of cyber-attack (Brasington & Park 2016).

The rapidly evolving nature of emerging technologies and growth in technology-based risks means that ports are severely challenged timewise in identifying, assessing and preparing for these risks (WEF 2018). This 'unknowable' challenge

also affects insurers, who, when unable to identify and estimate the likelihood, consequences and costs of cyber-attack and related risks, are unlikely to offer cover for this ambiguous category of risk, or to compensate for its consequences (Diebold, Doherty & Herring 2010). Whereas cyber-risk is a new and emerging risk that is likely to grow, ports encounter difficulties in obtaining adequate insurance cover for reasons of: 1) capped maximum policy value; 2) multiple policy exclusions; 3) indirect losses not covered; and, 4) policy complexities (Biener, Eling & Wirfs 2015).

Port infrastructure insurance has three primary foci (Rinaldi 2004; Nasiruzzaman, Pota & Islam 2011; Marsh 2014):

a) physical aspects of the damage involving clean-up and removal costs of non-repairable material, and subsequent repair and replacement;
b) reduced revenue stream and a consequential possibility of permanently losing customers and market share while either the port area is incapacitated, or port operations halt due to reliance upon incapacitated regional infrastructures (for example electrical power grid); and,
c) potential claims upon the port for liability compensation, including injury and/or damage, corporate liabilities, pollution cleanup, or industrial relations claims for workers compensation.

Critical infrastructure failure involving property damage or damage to plant and equipment are relatively common forms of insurable risk items (Rose & Huyck 2016) and from an insurer's perspective, the insurability process is relatively easy to identify and quantify (Kunreuther & Pauly 2009). In this research, respondents appear to be confident of insurance meeting recovery needs in consequence of infrastructure, plant and equipment damage or loss. Unplanned port shutdowns differ from shutdowns for planned maintenance reasons, because with the former, port managers and port users typically have very little or nil notice of the disruptive event that precipitates shutdown. Lam and Su (2015) establish that southern Asian and east Asian ports incur an increasing number of shutdowns from both natural disasters and labour stoppages from industrial strife. The effects

of a port shutdown might affect the adjoining regional economy, while the port is potentially exposed to financial losses, loss of business, and demurrage payments for ship delays (Mandaraka-Sheppard 2014; Rose & Wei 2013). Of note, port managers' expectations that their State-provided insurance would not cover an unplanned shutdown (Figure 7-8) is inconsistent with industry at large, which employs business interruption insurance against financial losses from issues with plant and equipment, failure of critical goods and services suppliers, or port-centric supply chain impediments (Rose & Huyck 2016).

The correlation coefficients between respondents' expectations for insurance coverage for differing risk categories are calculated to be primarily weak to moderate (for example .191 -> .493 using Kendall's TAU-*b* and Spearman's rho) and this variability and inconsistency suggests that their existing insurance coverages are not framed within a single pool of port authorities. An insurance pool consists of multiple similarly insured cases exposed to a common hazard, which permits insurers to control their level of exposure. They are enabled to do this through ability to predictively calculate the mean frequency and mean severity of potential losses (Dorfman & Cather 2012). Dorfman and Cather (2012) describe how organisations might consider paying an increased premium as a specified risk grows, but as the cost correspondingly escalates then organisations begin to drop out of the pool - particularly if they consider that a risk is of low probability.

Australian ports are geographically spread across seven State jurisdictions and insurance schemes, and individual states might not contemplate covering the risks of another state's ports. Also, whereas insurance pooling might be beneficial to Australian ports, Biener, Eling and Wirfs (2015) note in the context of insurable and uninsurable risks that incongruent risk characteristics preclude efficient insurer pooling. This is particularly so with small risk pools and dynamic hazards whose nature cannot be readily quantified. If this uninsured or uninsurable situation is the case with Australian ports, then in the absence of insurance the ports need to establish focused and effective mitigation strategies and risk management capabilities. As the Australian government suggests, insurance may

not be an entirely acceptable solution for critical infrastructure risk management problems (AG 2015).

7.7.2. Other studies on insurance coverage

In composite, port managers have mixed expectations of insurance coverage for the consequences of disruption, as shown in Figure 7-9. The reported least likely categories to be covered by insurance are unplanned shutdowns and industrial strife, and McNab (2015) describes these as common events in Australian ports. Risk characteristics and insurability of unplanned port shutdowns and industrial strife are examined by Lam and Su (2015) who conclude that insurance policies against major disruptions may be prohibitively expensive, if obtainable. Similarities exist between the impact and consequences of unplanned port shutdowns and the uncertainties of industrial strife - both are random disruptive events with unexpected occurrence (Gurning & Cahoon 2009; Lam & Su 2015).

7.8. Port hazards

Previously identified port hazards are reviewed from the perspectives of senior port executives, and these perspectives provide some insights into Australian port risk identification and vulnerability assessment processes. Multiple port hazards involve human causality from either an accidental or deliberate perspective, which leads the anthropogenic factor to become of multi-hazard/multi-risk concern for port managers (Kappes 2012; Gallina *et al*. 2016). The anthropogenic impact on the port risk environment is common to operations failure, security incidents, socio-political incidents, activism, financial risk, and crucial goods and services supplier failures. For these reasons, the human causality category of risk is discussed below within the context of its individual risks, rather than from a more challenging and complex multi-hazard and multi- level analysis perspective (Liu *et al*. 2015; Gimenez, Labaka & Hernantes 2017).

7.8.1. Operations failure – equipment, technology, ship accident

Port operations are dependent upon equipment, technology and systems employed by the ship or shore side of port operations (Burns 2015). One respondent comments that inhouse ability to cope with disruption is impaired

when the failure is related to 'critical services provided by external providers - maintenance that has been outsourced, IT services, outsourced HR recruitment'. This reliance on external providers and consequent vulnerability possibly relates to an external assistance requirement reported by five other respondents. Another respondent reported difficulty in managing disruptions that originates outside port-controlled land or waters, but with consequences that impact upon port operations. Again, this relates to vulnerability involving external parties and critical goods and services supply and a side issue relates to bringing specialist assistance to site. Delays in repairing failed or damaged equipment in remote areas was an issue noted by another port, whereby 'remote locality and limited access to sufficient technical expertise results in exacerbated delays'.

7.8.2. Security breaches

Security breaches, inclusive of sabotage, criminality, or cyber-attack are an increasing feature of 21st Century risk management and intuitively, this category is associated with disruptions of human causality (Rubin 1998; WEF 2018; AG 2017). When risks are viewed in order of coping difficulties, 'security' disruptions reportedly affect the least number of respondents, but conversely, the findings indicate that security breaches represent the most difficult type of risk to manage. Since the 2001 attacks upon US soil by Islamic terrorist group al-Qaeda, security became an increasingly specific focus of national and international critical infrastructure risk management (Baker-Beall, Heath-Kelly & Jarvis 2015). This focus eventually resulted in the formation of an Australian Department of Homeland Security (Viellaris & Osborne 2017). Other studies link counter-terrorism/radicalism hazards with those capable of harming ICT systems and operational/business dependencies upon cyber systems (Alcaraz & Zeadally 2015). This broadening of security focus incorporates Cloud data storage, computer usage, and data integrity, which researchers regard as crucial to the effectiveness of critical infrastructure operations and the utilisation of associated systems and equipment (Sookhak *et al*. 2017; Tucci 2017).

Sixty-five percent of respondents (*n* = 38, 65% = 25) experienced security breaches during the past five years, sufficient to affect the reliability of their port

operations, resources, capabilities and infrastructure. Forty percent (10) of these 25 respondents reported difficulties in coping with security breaches. These outcomes are addressed in non-parametric testing that found significant correlation and covariance when port risk management performance against security breaches is compared against the nine other disruption hazards reviewed.

7.8.3. Adverse natural events

Increasingly severe weather events, plus resultant storm surge and floods pose a seasonal threat to Australian port operations. Ports in northern Australia are subject to cyclones, while southern ports are vulnerable to storm fronts, southerly lows, hail and electrical storms (Ng *et al.* 2013a; Allen, Karoly & Walsh 2014; Walsh *et al.* 2016). Respondents report on their abilities to manage adverse natural events during the past five years (n = 39). Seven were unable to cope when a disruption overwhelmed their response capabilities, for example a cyclone that impacted north Queensland closed multiple ports until severe flooding receded and repairs became possible (Tracey 2011). Twenty-seven respondents reported that they effectively managed all adverse weather events. Five others reported that they had not experienced adverse natural events during the past five years. Some port managers acknowledge the inevitability of harm arising from natural events, and pre-emptive port closure action is taken by managers accustomed to cyclonic weather patterns. This weather-related port shut-down process is adaptable to ports outside the cyclone zone, for example Flinders Ports in South Australia employed pre-emptive port closure in managing the onset of a severe storm (Kavina 2017, np):

> When long-range weather forecasts showed that a super-storm was heading for South Australia, Flinders Ports activated its safety management plan for adverse weather. The storm posed a major hazard to people and assets, so Flinders Ports took the unprecedented step of closing all seven of its ports for 48-hours, when the storm battered the State at the end of September… No-one was injured and there was no major damage to our assets or equipment at any of our ports. Being prepared and making safety the top priority was the key to a positive outcome.

7.8.3.1. Climate change - a multi-risk assessment approach

Respondents appear to have low expectations of climate change hazards for the future; quantitative data indicates that climate change consequences are of least concern to port managers, with only seven of thirty-eight acknowledging such disruptions as very likely, and five as somewhat likely. Qualitatively, even weaker opinion emerges, when from two separate questions only one respondent reports climate change as a likely hazard. The impact and manifestation of climate change consequences is said to exacerbate the severity of adverse natural events – for example storms, floods and droughts (Gallina *et al.* 2016). Climate change is regarded as either a multi-hazard risk or a multi-risk concept that encompasses the total risk from multiple hazards (Kappes *et al.* 2012; Garcia-Aristizabal & Marzocchi 2015; Gallina *et al.* 2016). Kappes *et al*. (2012) describe the multi-hazard challenges and complexities in visualising and ranking the large quantity of information related to natural hazards or risks. For these reason, Gallina *et al*. (2016, p. 123) argue that:

> Usually a hazard by hazard approach is considered for evaluating the consequences of individual natural and climate related hazards (e.g. heavy precipitation events, droughts, floods, debris flows, landslides, storm surges) on vulnerable systems.

From a multi-risk perspective, climate change within this thesis is regarded as a generic risk, or category of risk rather than a specific risk event. A detailed multi-hazards study of climate change and its influences upon Australian ports is beyond the scope of this study. For this reason, climate change was disregarded from the analysis.

7.8.4. Socio-political disruptions

Socio-political risks have far-reaching potential to impact organisations, systems, and risk management thinking and behaviour. This category of risk might arise from multiple sources, for example, government intervention, public and local community anti-industry sentiment, environmental activists, corruption, and deliberate harmful acts (Bekefi & Epstein 2006; Connor 2012). Organisational

abilities to identify and assess these social and political hazards can be shaped by how managers perceive risks and uncertainties (Assmuth, Hildén & Benighaus 2010; Strang, Korstanje & Vajjhala 2018). Australian ports are subject to diverse socio-political risks and disruptions related to their onshore and offshore operational interests, including changes in political decisions, community opposition, strikes, protests, radicalism, seabed boundary disputes, ocean resource disputes, radicalisation of disaffected persons (Paton, Kelly & Doherty 2006; Guild 2009; Dauvergne & LeBaron 2014; Kaye 2015; Anton 2017; Boin, 't Hart, Stern & Sundelius 2017). Respondents reported that political reforms, changes and interventions were of increasing concern now and for the future, particularly in relation to port reform, regulation and privatisation. Self-reported abilities to cope with diverse socio-political risks are shown in Table 7-4.

Disruption category	**Coped well**	**Barely coped**	**Unable to cope**	**Required external assistance**	**Unsure**	**Not applicable**
Socio-political intervention or IR issues	18= 46.2%	7= 17.9%	1= 2.6%	0	3= 7.7%	10= 25.6%

Table 7-4: Port abilities for coping with socio-political disruptions (Author).

Twenty-nine respondents encountered socio-political disruptions and of these seven barely coped, three were unsure about how well their situations were resolved, and one organisation was unable to cope. In trying to understand the reasons for the difficulties in managing this risk, the research turned to Everett (2003) who argues that State government port owners might apply informal political interference (Ministerial and departmental) in port management. Bailey and Peetz (2014) describe industrial relations situations at some Australian resource export ports as 'volatile' and port managers are known to be frequently challenged by industrial relations, social activism and port reform risks (Pigna 2014; Davidson 2016; Toscano 2016). Other studies indicate that improvements in this aspect of hazard management might arise with better understandings of human motivation for engaging in deliberate adverse acts, sabotage, criminality, terrorism, activism, threatening behaviour, and issue-oriented violence (Vanderheiden 2008; Borum & Neer 2017). In the case of ports, such an

understanding might motivate the preparation of hazard-specific mitigation and response strategies and techniques.

7.8.5. Financial risk

Port financial risks, as with other organisations, might arise from cost overspend, fraud, theft, data theft, record keeping and storage safety, financial instability, banking transaction failure, or financial information discrepancies (Shiller 2009). Financial disruption might also be consequential to disruptions involving other factors with potential to impact port business or customers. Findings of this research indicate that the possibility of financial disruption can be associated with that of commercial and political risk - not surprisingly so, since Australian port finances are derived from commercial transactions and capital expenditure requires State government approvals (Birrell 2016). Of thirty-nine respondents, 27 reported experiencing financial problems during the past five years, with 20.5% (8) not coping well, and a further two ports required external assistance. Sufficient qualitative information from thirteen of thirty-nine respondents establishes an association between financial risk, socio-political and commercial risk. Survey respondents reported in open-ended answers that:

1) ‘There is a challenging economic outlook’;
2) ‘Access to capital has become more difficult due to the State Government's budget challenges. I expect pressure will only increase in coming years’;
3) ‘Lack of budget by State government’;
4) ‘Trade is unreliable, funding is hard to come by or have committed due to the unreliable trade’;
5) Loss of business due to shipping industry downturns’;
6) ‘Revenue reduction – supply chains seeking diversification of services products (and) sourcing new markets for services’; and,
7) ‘The industry has been going through a difficult downturn over the last 3 years’.

Financial disruption whether as a singular risk, or as the consequence of other types of disruption, is shown by the respondent reports to be a port issue of high concern.

7.8.6. Information communications and technology

Business continuity management requires port data backup capabilities plus availability of an alternate communications, data and records system that is regularly updated from daily records. The Business Continuity Institute (BCI 2008, Section 3, p. 5) argues the necessity for ensuring that:

> Electronic and other records are duplicated at another geographically separated location in a form that allows them to be accessible and recovered for use within business-defined timescales.

Port communications in their many forms are crucial to the success or failure of multiple processes. These include ongoing operations, business relationships and contractual arrangements, enablement of critical goods and services, emergency management, and community engagement (Cahoon 2004). The port's information and communications systems enable ports to monitor frontline and support processes, plus the external supply chain environment, for potential points of failure or inefficient practices (Cahoon 2004). Weick and Sutcliffe (2015) describe this process as 'organisational mindfulness' towards early warning against unexpected disruptions. Disruption to the port's communications system carries broad adverse implications for all aspects of intermodal operations, and the respondents' ability to cope with past disruption to communications systems and services is shown in Table 7-5.

Disruption category	Coped effectively	Barely coped	Unsure	Required external assistance	Not applicable
Communications systems and services	21= 53.8%	5= 12.8%	4= 10.3%	4= 10.3%	4= 10.3%

Table 7-5: Abilities to cope with communications systems and/or services failure (Author).

The port is reliant on externally located critical goods and services providers for its telecommunications, internet services and ICT infrastructure. Respondents acknowledge that disruption to these providers readily impacts port operations, for example loss of ability to transact electronic documentation or to arrange shipping operations with ship agents and freight forwarders (Cahoon 2004). Internal communication systems, and potential for silo management were also

problematic to port managers, where ‘it is not so much an issue with not being able to cope with a particular event, we find issues around communication to be our biggest hindrance (related to people's training and preparedness)’.

Information and communications technology systems (ICT) are additionally at risk to deliberate harmful intent involved with cyber-threats, an increasingly likely risk for port operations (Renn 2014; WEF 2018). ICT equipment and systems form part of a port’s infrastructure and superstructure, inclusive of dedicated computer systems that are drivers and controllers of port plant and equipment (Burns 2015). According to one respondent, Australian port ICT systems reliability is viewed ‘not only as a technological process, human involvement can be an exacerbating issue’.

7.8.7. Infrastructure failure

Port vulnerabilities arising from infrastructure failure might have multiple causes (Dueñas-Osorio & Vemuru 2009; Urlainis *et al*. 2014; Pescaroli & Alexander 2016). This thesis finds that port infrastructure disruption has extensivey challenged respondents, with 28.3% either barely coping, requiring external assistance, or being unsure of how effective eventual recovery was to normal operations, as shown in Table 7-6. Qualitative responses reveal that concern is felt about the reliability of external infrastructure upon which external goods and services suppliers are reliant. Infrastructure reliability requires frequent maintenance, repair and replacement (Tsinker 2004) and several of the respondents express their concerns about State government constraints in the use of operational and capital expenditure on these works. Port authority managers are, to varying extents, reliant upon State government approval to spend money on infrastructure repair and maintenance. They are also controlled by State government fee regulations in what they can charge port users to utilise this infrastructure, for example harbour dues and wharfage (Everett 2007; Bandara & Nguyen 2015). The financing of port infrastructure disruption recovery may also be more problematical for port authority managers than for privatised port or terminal operators.

Disruption category	Coped effectively	Barely coped	Neutral	Required external assistance	Unable to cope	Not applicable
Infrastructure failure – internal or external locations	24=61.5%	6= 15.4%	1= 2.6%	4= 10.3%	0	4= 10.3%

Table 7-6: Ability of respondents to cope with Infrastructure failure: n= 39.

Recovery from infrastructure failure is also made complex because replacing key items like gantry cranes at a container port involves long lead times, due to sourcing from overseas. Notteboom (2007) notes that the Chinese manufacturer ZPMC is the predominant global gantry crane supplier and typically carries full order books. As previously discussed, respondents are unsure whether insurance will cover the repair or replacement costs of damage to port-centric infrastructure. Qualitative data gathered in Q6 provides a degree of association between port management concerns about economic stress, aging infrastructure, insufficient funds for infrastructure maintenance, plus a decreasing ability of State governments to assist in capital funding requirements.

7.8.8. Environmental disruptions

Port managers are challenged in their environmental management and sustainability capabilities and capacities, due to the multitude of port users, leaseholders, service providers and community recreational users whose interactions with port processes and activities add to the cumulative port risks of environmental harm (Rondinelli & Berry 2000; Dinwoodie, Tuck & Knowles 2012; Lam & Lai 2015). These challenges contribute to Australian port managers' past difficulties in coping with environmental disruptions as shown in Table 7-7.

Disruption category	Coped effectively	Barely coped	Neutral	Required external assistance	Unable to cope	Not applicable
Environmental causality	26= 66.7%	2= 5.1%	2= 5.1%	3= 7.7%	0	6= 15.4%

Table 7-7: Ability of respondents to cope with environmental disruption to operations.

Environmental disruptions are relatively commonplace, with eighty four percent of respondents experiencing environmental incidents at their ports during the past five years. Environmental incidents are heavily regulated with a proliferation of

State and national government regulatory measures, industry codes of conduct, plus public and private sector pressures for increased environmental sustainability within the port industry (Acciaro *et al*. 2014; Puig, Wooldridge & Darbra 2014; Di Vaio & Varriale 2018). Arguably, port management capabilities in managing environmental issues become a public 'face' of the port, and from a sustainability perspective, port managers need to consider the impact and image of port operations upon the local community and wider society. Respondents comment upon environmental activist risk, and an important risk management consideration might be towards prevention and mitigation of environmental problems, to minimise potential for socio-political consequences and reputational harm.

Unexpectedly, the qualitative data gathered from this survey provides little evidence of port management concern about future 'environmental' and 'adverse natural event' risks whereas the quantitative data indicates otherwise.

7.8.9. Crucial goods and services supplier failure

This section examines Australian port capabilities and capacities in managing critical goods and services provider downtime, with port coping experiences shown in Table 7-8 (*n* = 39). Crucial goods and services suppliers are a key element in maintaining port operations business continuity and the effectiveness of port operational performance (Waidringer & Lumsden 1998; Gurning & Cahoon 2011a; Thai & Chen 2011; MacKenzie 2012). When Cyclone Debbie floods severely impacted critical supporting infrastructure of Queensland ports, the ports lost hinterland road and rail connectivity, plus their access to goods and services suppliers and customers (Lam 2017; Reynolds 2017). Consequently, ports waited upon recoveries of crucial goods and services suppliers' infrastructure and superstructure before port operations could resume (Reynolds 2017). A similar event and recovery delay while waiting on external stakeholder recoveries was experienced by the US Port of NYNJ following the consequences of Hurricane Sandy (Wakeman 2013).

Disruption category	Coped effectively	Barely coped	Neutral	Required external assistance	Not applicable
Crucial goods and services supplier failure	19= 48.7%	5= 12.8%	3= 7.7%	4= 10.3%	8= 20.5%

Table 7-8: Port effectiveness in coping with critical goods and services provider failure (Author).

The survey revealed that across all categories of port disruption management, loss of crucial goods and services supply demonstrated the highest requirement for external assistance. This might be expected since crucial goods and services suppliers are primarily organisations located external to the port, and replacement of these providers requires managers to source alternative external suppliers (if available).

7.9. Identifying future hazards

A comparison was performed earlier in this chapter between port managers perceptions of past disruptions and their expectations for these disruption categories to recur in the future (S 7.4.3.). The association between these categorical variables was evaluated by a Chi-square test for independence and is now evaluated through qualitative means.

7.9.1. Qualitative analysis of future risk predictions

Respondents' expectations of risks to arise during the next five years are acquired in free-form format from Q7 (*n*= 38) and Q12 (*n*= 31), and qualitative analysis performed with Dedoose software as shown in Figure 7-9. As with the quantitative data acquired from closed questions, socio-political risk figures prominently, followed by financial, technology changes and commercial risks. The scale of response is colour coded to establish the relative strengths of co-occurrence between various code inputs, with red the highest indicator (Talanquer 2014).

Media \ Codes	Climate change	Commercial risks	Critical goods and services	Cyber threat	Disruption management shortfalls	Environmental risks	Finance	Human causality	Infrastructure	Natural events	Personnel management issues	Ship accidents	Socio-political risk	Technology - rapid pace of change	Totals
Q12 qualitative future risks.docx		3		3	7	2	9	1	3		9		18	13	68
Future threats.docx	1	16	6	1		2	13	9	7	2		9	7	8	81
Totals	1	19	6	4	7	4	22	10	10	2	9	9	25	21	

Figure 7-9: Qualitative comparative analysis of respondent predictions for future risks (Author).

Multiple respondents to Q12 expressed their concern about the impacts of port reform and privatisation upon port management, concurrent consequences of reducing finances, and a loss of control and authority in their regulatory tasks. This occurs concurrently with national and State governments increasing port regulatory roles, responsibilities and complexities (Chen & Everett 2014). Port management responsibilities for maintaining ageing infrastructure, plant and equipment in an era of financial constraints was of widespread respondent concern. The rapid pace of technology change gives rise to potential future problems in coping with increasing vessel sizes, and one manager raised the possibility of having to finance the provision of LNG fuel bunkering facilities for new construction vessels. Internal staff abilities to cope with rapid technology change was questioned by five respondents, and a common concern was raised that in a time of personnel downsizing, the rate of data throughput and complexity of operations within ports are increasing. The possibility of automation to perform pilotage and towage tasks and/or leading towards crewless vessels was raised as a potential source of concern by six respondents, but without discussion of any likely consequences of failure.

Concerns about political influences upon port management functions and 'further changes to Port Authorities roles and responsibilities' are revealing, for example one respondent comment is that:

> Fragmentation of emergency responsibilities between multiple government departments and authorities may inhibit an effective co-ordinated

> emergency response. Our organisation is too small to fill that potential response void.

Another respondent observed that 'increasing governance and external control is introducing bureaucracy that a medium sized company has limited resources to support' while another noted that 'Government changes introduce uncertainty in emergency management procedures and command and control arrangements'. Steele, Hussey and Dovers (2017) argue that apportioning risk management roles and responsibilities across partially government/partially private sector critical infrastructure agencies is problematic, and particularly so in dealing with the risks of new and emerging hazard events.

Respondent concerns about government risk management change initiatives might arise from Australian government efforts to break down 'established, and sometimes entrenched, boundaries between agencies, sectors and levels of operation' that might impede an increase in critical infrastructure resilience (Rogers 2011, p. 55). At this comparatively early phase of critical infrastructure resilience planning (AG 2017), potential exists for some port managers to be unaware of government resilience plans and intentions, while government planners might not be cognisant of port management risk management capability limitations, or of any port management unawareness of national resilience plans and inaugurating processes.

In summation, the findings suggest that port managers are aware of new and emerging risk challenges, and that these new challenges might arise within operational, socio-political, technology, commercial and financial contexts.

7.9.2. Business continuity preparedness

Q13 employs a Yes/No format to ascertain whether respondents (*n*= 38) have instigated five business continuity preparedness factors identified by Hiles (2011). The findings (Figure 7-10) suggest that respondents are generally aware of what core operational capabilities are necessary for effective business continuity. They are less cognisant of the longest tolerable period of operational downtime they might have for disruption recovery, or of how effective their emergency

operations centre might be in the absence of normal operational premises and systems.

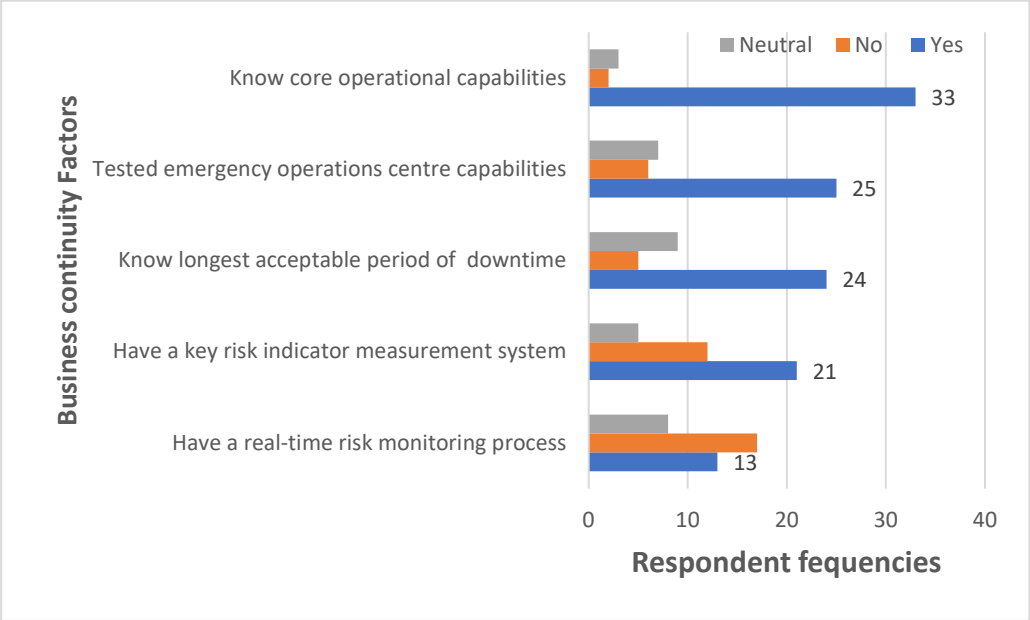


Figure 7-10: Preparedness for port business continuity (Author).

Few respondents (13: 34.2%) have established a real-time risk monitoring system, despite key risk indicators, like key performance indicators, being a well-established tool to establish the effectiveness of operational risk management performance (Scandizzo 2005; Gaudenzi & Borghesi 2006). Only twenty-one respondents (55%) had implemented such a system and mapped their key risk indicators.

7.9.3. Transition from 'business as usual' to disruption management mode

Q14 qualitatively explores how management prepares port employees to switch quickly from 'business as usual' to a disruption management mode of operations (n = 35). Table 7-9 illustrates that five respondents acknowledge significant deficiencies within their business continuity preparations, while others report low levels of disruption management preparedness. Four reports on insufficiency of employee training and exercises include:

a) 'The port should conduct sufficient contingency trials and exercises. however, the terminal operator does not have the expertise or desire to undertake these necessary activities';

b) ‘We run desk top exercises, but we need to run more on the ground exercises’;

c) From a port reform perspective one respondent reports that: ‘We no longer have port employees’; and, more succinctly,

d) ‘We don’t’.

Business continuity factor	Respondent reports
Acknowledged business continuity inadequacies	5
Training and exercises	23
Strategies and plans in place or in progress	19
Engaged workforce	4
Communications and leadership	3
Dedicated business continuity team	3
Collaboration with external entities	3
Business resilience program in progress	1
Ongoing vulnerability assessments	1
Total reports:	62

Table 7-9: Port business continuity preparedness measures (Author).

Twenty-three respondents describe their training and exercise regimes, which vary from desktop drills through to onsite scenario-based exercises. The survey questionnaire apparently reached one manager at a time when the port was reviewing its disruption management program; the manager comments that:

> Part of our new framework that will be rolled out in the next few months - we have an extensive training and exercising program being established. We have also developed port continuity plans (which will) assist with quick decision making by providing matrices to pre-evaluated scenarios. We are also working with our stakeholders to ensure infrastructure is suited to meet their requirements in the event of a disruption.

Port managers’ training and exercise programs encompass key disruption management components of response, management and recovery with one respondent noting that staff undertake: ‘Training in incident management, business continuity and crisis management, (provided by) drills and practice’. Others note the importance of: ‘Training and empowering’; ‘Training and drills for emergency response plans’; and, more emphatically, ‘Training exercises, and more training exercises’. Signs of a positive risk management culture emerge with comments of: ‘Training and good leadership’; ‘Training and empowering’; ‘In-

house emergency response training combined with ports current can do attitude'; 'Good communications and leadership'; 'Good procedures and regular exercises'; 'An engaged workforce'; and, 'Procedures and responsibilities for tasks required to keep the business running or to get it back up and running are documented, discussed and tested'.

7.9.4. Small ports' disruption management preparedness

The marine publication Guide to Port Entry (Witherby 2018) indicates that at least twenty single operator ports, terminals and installations are located either on the Australian mainland, at Australian territorial or external territory islands, or at offshore installations within Australia's exclusive economic zone. Little is known about the disruption management capabilities of these smaller Australian port organisations, consisting of single operator ports, terminals or offshore installations. One respondent noting that a terminal operator '…does not have the expertise or desire to undertake these necessary activities' is suggestive of a safety culture mindset that regards risk management as someone else's responsibility. Two of Australia's largest port fires and hydrocarbon releases occurred at single operator offshore facilities, and both incidents required extensive external disruption management assistance (Bower-White 2012). A comparison between small port risk management processes and those of large ports appears to be worthy of future research but is beyond the scope of this study.

7.9.5. Scheduling emergency management training, drills and exercises

Australia's national security and emergency management preparedness is based upon the Sendai Framework for Disaster Risk Reduction 2015:2030, and Emergency Management Australia (EMA) is a division within the national Attorney-General's Department with responsibilities for national security and emergency management capability. The Australian Emergency Planning Manual 43 (EMA 2004) notes that emergency management training and exercises perform an important role in testing plans and capabilities, and in maintaining organisational awareness of risk throughout extended periods of minimal crisis. Further, emergency and business continuity exercises are essential to testing plans following changes affecting either staffing, operations, or the risk environment.

Other reasons for training, drills and exercises include enhancing managers' communications, coordination and collaboration skills on an internal basis, and externally, to test management skills, capabilities, capacities and resources sharing with regional emergency management entities under simulated emergency conditions. Respondents indicate that their emergency management preparedness generally evolve around a framework that reflects EMA guidelines. Port emergency management teams also participate in national strategic and operational oil spill training exercises, for example Exercise Westwind in 2015 and Exercise van Diemen in 2016 (AMSA 2018). A sequential emergency preparedness framework is prepared from an interpretation of respondent reports as shown in Figure 7-11.

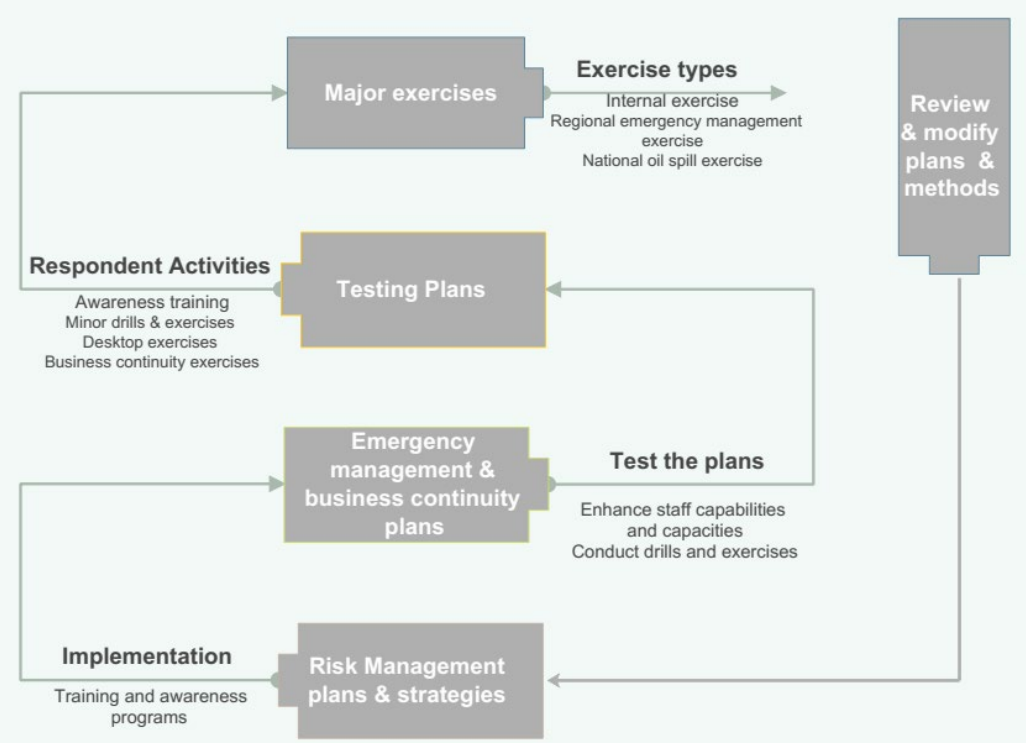


Figure 7-11: Port emergency preparedness framework (Author).

One port's contingency training follows a formal framework:

> Emergency response is conducted at least monthly, crisis management at least twice a year, (and) desktop exercises at least monthly.

Another respondent reports a 'bottom up' training format that potentially might be improved with top-down participation:

> Operationally - emergency response exercises, fire, and oil, and security drills partially address leading edges of disruption but there has been no full disruption training involving the full executive and or Board.

The reported frequency of emergency management and business continuity training (*n*= 37) provides interesting information on the dichotomy between managers reporting nil disruption training (6= 16.2%) and those who schedule training sessions quarterly or more (10= 27%). The response spread is shown in Figure 7-12. One outlier respondent reported that their port conducted disruption training at three-yearly intervals but gave no reason for this frequency. Drills and exercises are part of the port training system, in which drills are practised regularly to test specific emergency capabilities or functions (firefighting, first aid, security response) whereas exercises are held at longer intervals to test and review knowledge, capabilities, capacities, personnel availability, and adequacy of resources (Haddow, Bullock & Coppola 2017). In summation, annual disruption response training is preferred by the largest group of port managers (14= 37.8%) however a slightly larger group adheres to a more rigorous training routine of multiple sessions each year (17= 45.9%). The minority group reporting nil disruption training is suggestive of an Australian critical infrastructure vulnerability. Mindset change towards such training potentially offers opportunity for a low-cost improvement to port sector risk management effectiveness.

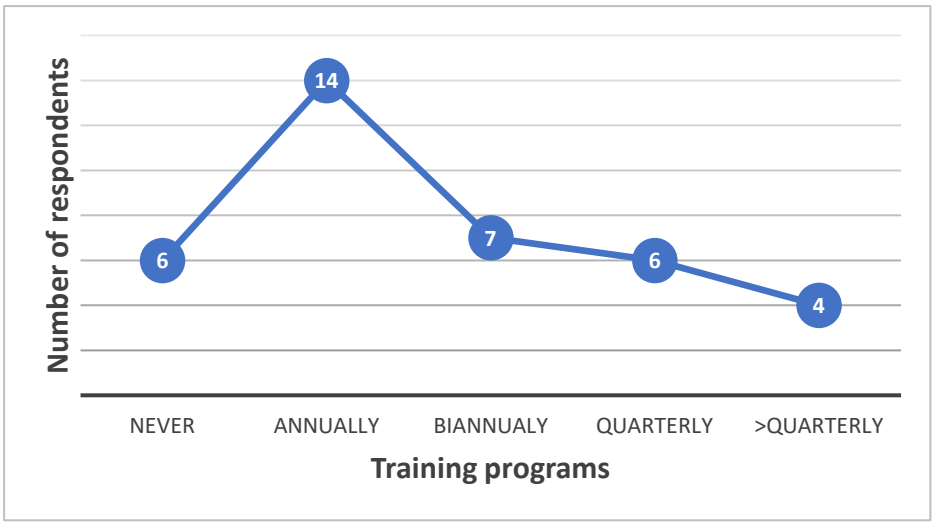


Figure 7-12: Frequency of port emergency management training programs (Author).

With port authorities increasingly managing multiple ports (either under direct government departmental auspices or because of port reform and amalgamation) one respondent noted that the number and types of disruption response training varies from port to port under the port authority's regulatory control.

7.10. Disruption responses

This section of the data analysis explores port perceptions about maintaining operational services during and following a disruptive event from Questions 16, 17 and 18 which provide quantitative and qualitative data related to questions arising from the literature review.

7.10.1. Assets and services

Respondents' opinions in Q16 (*n* = 36) were tested with a frequency analysis (outputs shown in Figure 7-13) for importance of port assets and services in support of business continuity. The port's core business continuity reliance rests internally with its plant and equipment, ICT systems, electrical power and key personnel. External support inputs (reported as lower albeit essential priorities) are: 1) transportation services, 2) water and waste water services, 3) critical goods and services supply, and 4) fuel.

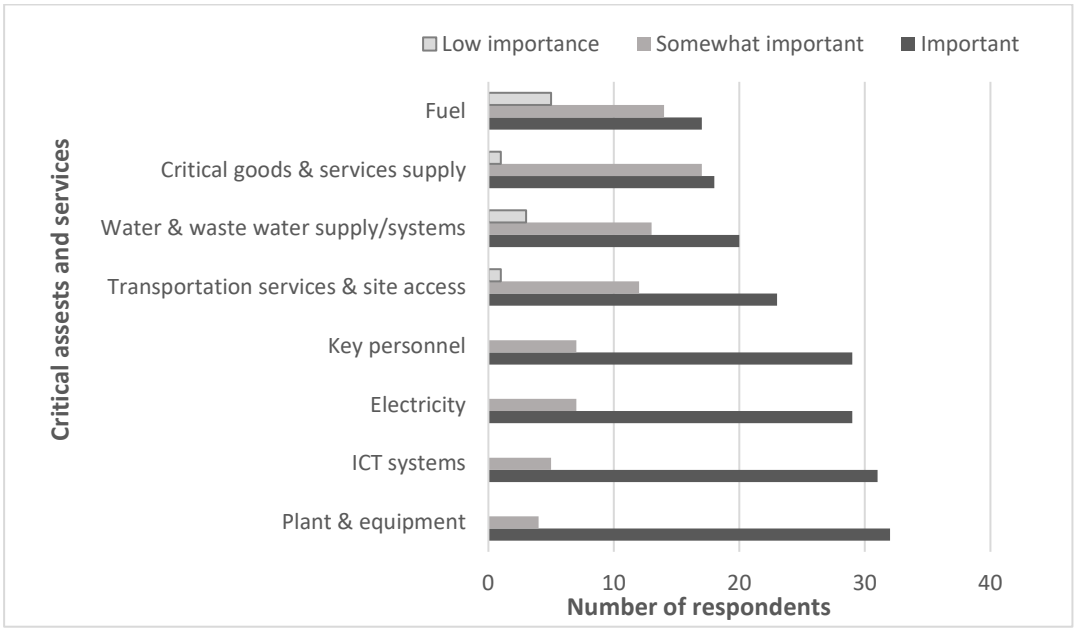


Figure 7-13: Port assets and services critical to operational business continuity (Author).

Respondents free-form notes accompanying Q16 include acknowledgement that port assets and services 'are not just important, but crucial' to business continuity, and that other essential services include 'internet, phone network (mobile or land line), wharf infrastructure and stevedoring staff'.

7.10.2. Maintaining business continuity

This section investigates port risk management preparedness, and particularly management capabilities and capacities towards maintaining business continuity. Some factors crucial to global port operations were identified from the literature (Alderton 2013; Burns 2015; Bichou 2018) and these were tested against management responses to evaluate their relevance to Australian port requirements. Results are shown in Figure 7-14, indicating the value of respondent concerns for the continued availability of plant and equipment, key personnel and ICT systems. From an internal perspective, if the port has these three factors in service then in the short term at least, they continue to be capable of working cargo and port systems. In the longer term, the non-availability of other crucial inputs to port operations might constrain intermodal operations continuity. This issue is explored in the next section which evaluates the respondents' regard for the availability of other assets and services.

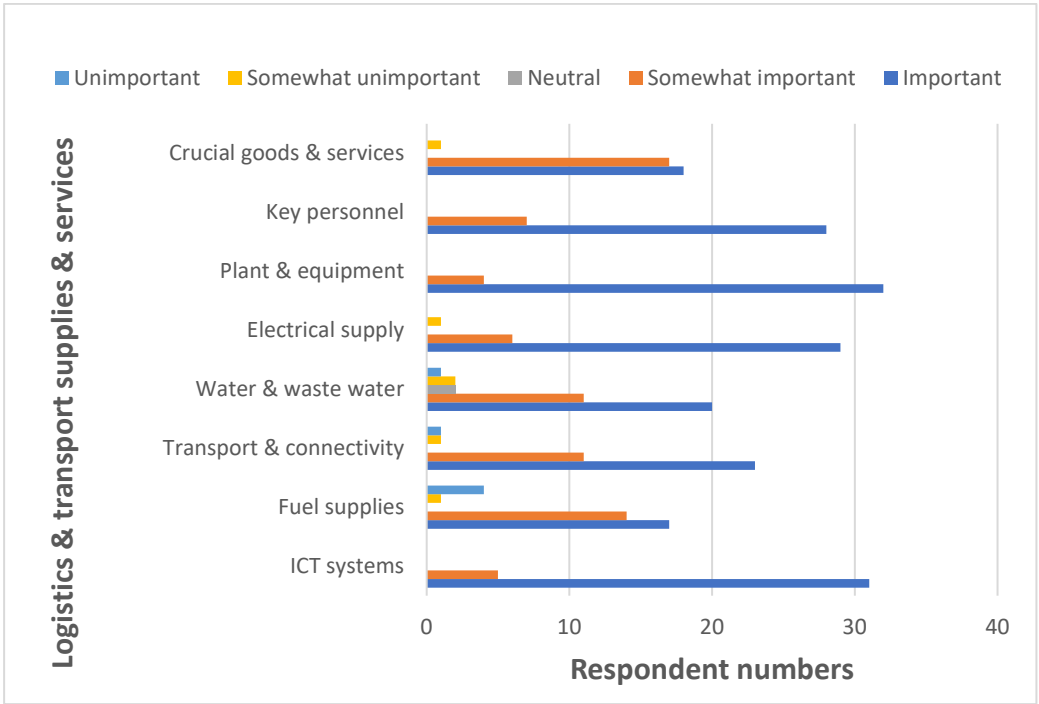


Figure 7-14:Port business continuity reliance on logistics and transportation inputs (Author).

Port vulnerability assessments within an intermodal business continuity context involve identification of key capabilities and enabling requirements (Hsieh, Tai & Lee 2014; Pitilakis *et al.* 2016). Managers must identify actors, assets, resources and infrastructure that are crucial to the port operations task, and what requirements are necessary to maintain these primary support capabilities (Schnaubelt, Larson & Boyer 2014). To maintain port business continuity, managers need to identify what underpins their operations in the short and longer terms and to prepare against these crucial requirements becoming failure points. These crucial requirements include assets and services, and respondents' concern for some aspects of this area of operations is shown in Figure 7-15.

Maintaining contact lists for emergency agency contacts was the most highly regarded factor, suggestive that managers are primarily motivated towards what is needed at the onset of a disruption, and less concerned for measures (albeit still important) to be called in at a later stage of business continuity response.

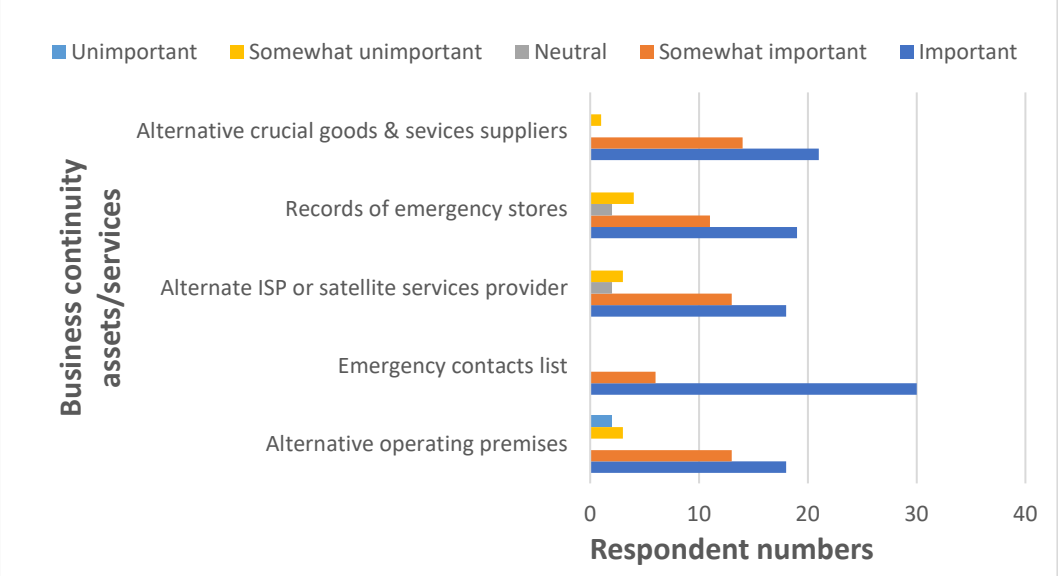


Figure 7-15: Port business continuity regard for assets and services (Author).

Eleven respondents provided free-form indications of risk management qualities of importance to business continuity, inclusive of flexibility, adaptiveness, and preparedness which accord with the primary attributes of critical infrastructure resilience (ISO 22316: 2017; Wei, Chen & Rose 2017). Respondent reports on business continuity requirements include:

a) (We have) three ports and city corporate office, there is sufficient redundancy for alternative operating premises. That said we have alternative sites earmarked;
b) Ensuring all personnel are familiar with emergency management protocols and procedures. Ensuring Key Personnel remain current in contemporary emergency management assessment processes and procedures;
c) Ability to work from anywhere; and,
d) Ensuring all personnel are familiar with emergency management protocols and procedures. Ensuring Key Personnel remain current in contemporary emergency management assessment processes and procedures.

Figure 7-16 is a composite of respondent qualitative responses enabled by Dedoose software, to indicate that highest qualitative regard towards business continuity capabilities is for availability of apparatus: backup generators; oil/chemical spill response items; firefighting equipment; and command, control and communications items; and, an ICT system backup battery. Essential supplies were next priority, with requirements for onsite water and fuel reserves, and rescue/medical items and equipment. Third priority was for trailer mounted tower lights for emergency illumination. Minor priority was regarded to offsite or cloud data backup, and somewhat surprisingly, for staff preparedness - which might be expected to have higher priority given the importance attached to key personnel as shown in Figure 7-16.

Media \ Codes	Alternative sites identified	Backup generator	Command & Control equipment	Competent and trained staff	Emergency lighting trailers	Equipment redundancies	Firefighting equipment	Flexibility and adaptiveness	ICT Systems battery bank	Offsite data backup	Oil/Chemical spill response	On site fuel reserves	On site potable water reserves	Preparedness	Rescue & medical equipment	Totals
Q18 Disruption Management	1	30	23	3	15		26		24	3	30	21	21	2	19	218
Q17 Qualitative.docx	1					3		7						7		18
Totals	2	30	23	3	15	3	26	7	24	3	30	21	21	9	19	

Figure 7-16: Respondents free-form responses regarding business continuity support (Author).

7.11. Summary of port risk management findings

Within the testing sample (n = 37), senior Australian port executives are generally experienced in their roles with 84% having more than three years tenure. Five of these managers lack risk management qualifications, whereas others held multiple combinations of academic and commercial risk management certifications (Section 7.4.). Thirteen managers had not experienced port disruptions, however twenty-eight reported that their ports held periodical drills and major emergency management exercises (Section 7.9.5.) Risks that concern port managers most are reported as adverse natural events; business-oriented risk, with loss of customers and competition; financial constraints, socio-political interventions or restrictions; and, disruptions of human causality.

The primary research question is partially addressed by respondent reporting their experiences in managing disruptions during the past five years in terms of responding, managing and recovering from disruptions (Section 7.5.).

Australian port risk management capabilities and competencies are uneven, and the evidence suggests that port risk and security management improvements would be beneficial. The research findings on port abilities to cope with disruptions (Sections 7.5.; 7.6.) suggest in general that:

a) Australian ports demonstrate mixed levels of effectiveness in managing the risks and consequences arising from low probability/high consequence disruptions.

b) Australian port disruption management capabilities appear, in general, to be based on sound risk management principles as evidenced by management abilities to cope.

c) Australian ports appear to be better prepared to manage physically manifested disruptions, for example storms, oil and chemical spills, and infrastructure damage than less tangible hazards, for example security breaches, cyber-threat, criminality, and socio-political acts.

d) Ports vary widely in their capacity and willingness to train for and prepare for disruptions, with one port reportedly ignoring this practice, and another lacking the personnel to undertake emergency management processes. Multiple ports demonstrate a strong and comprehensive commitment to risk management and emergency management training (Subsections 8.3.2.; 7.9.5.).

e) Port reform and asset sale processes are reported to decrease port management controls over port land and infrastructure usage, plus reduce economic viabilities and staff numbers, which together act to diminish disruption management capabilities (Subsections 7.9.1.; 7.9.3.).

The literature provides little in the way of a port disruption management performance benchmark, against which this study's findings might be compared. Additionally, disruption severities and port circumstances will likely vary from port to port to such an extent that benchmarking might only be an approximate measure. In the absence of other studies to provide a suitable benchmark for comparison, there is little to say on whether Australian ports presently fare better or worse in this regard than their global counterparts. As discussed in Section 7.6., the findings suggest that some Australian ports have potential for improvement in managing future port hazards associated with high levels of uncertainty, unpredictability and indeterminate levels of severity.

Port managers indicate their beliefs that the frequency of disruptions will decrease in the future, whereas a body of research and global surveys indicates that the opposite is more likely (Subsection 7.5.1.). Port managers' reports of past

disruptions and the frequencies of their expectations for future disruptions are statistically different, and three potential explanations (or a combination of these explanations) might contribute to this finding. Either the pattern of disruption types is changing, risk mitigation or avoidance of risks is becoming effective, or a possibility exists that port managers understanding of future risk frequencies is flawed – for example from lack of knowledge or deliberate risk myopia. If managers translate their understanding of a reduced risk environment into the risk assessment process, then a possibility exists that some Australian ports may be under-prepared when responding to future disruption events. From a strategic perspective, if port managers wrongly believe that certain hazards are less likely in the future, then a possibility exists that risk management resources and assets are mistakenly being allocated to other areas.

Managers have concerns about ageing infrastructure and budgetary constraints upon maintenance and capital works (Section 7.5.). This suggests that port infrastructure failure may become a more common hazard, with respondents indicating that they are currently experiencing difficulties in managing the consequences of reduced infrastructure maintenance (Subsection 7.8.7.).

As port abilities to accumulate cash reserves and precautionary savings towards infrastructure failure or disruption recovery become constrained (Subsection 7.8.5.) then the role of insurance becomes more important. Port managers report that while insurance is an effective means of transferring risk, they are unlikely to utilise insurance to the partial exclusion of other risk mitigation strategies and processes (Section 7.7.). They recognise that insurance cover does not obviate their roles and responsibilities for monitoring, mitigating and managing the risk event. When port managers take up insurance, port risk insurability represents risks that insurers regard as tangible and measurable, and premiums that ports can afford. Respondents note, however, that as disruption categories and consequences become more unclear and uncertain, port risk insurability reduces as insurer reluctance increases. If a category of risk becomes uninsurable then port managers will need to strengthen their preparedness to treat that vulnerability. Freeman (2017) finds from academic and practitioner perspectives that decision-

makers operating in a risk-prone environment are inevitably exposed to uninsurable risks, and that this experience serves to heighten organisational risk aversion.

Australian port managers' uncertainties about managing future risks (Subsection 7.5.2.; Section 7.6.; Section 7.8.) potentially impedes their preparedness for managing the risks and consequences of low probability/high consequence disruptions. Their vulnerability assessments have difficulty in conceptualising external party interventions, either intentional (as with socio-political or criminality risks) or unintended (potential failure of critical goods and services supply). However, port managers do recognise that the risk environment is changing, and that new and emerging port risks, plus increasingly severe natural events, increase their vulnerabilities to business continuity failures (Section 7.8.).

7.12. An integrated and systematic approach to managing risk

An important finding from the risk management component of the survey is that the current risk management state reflects a 69.24% (statistical mean) of Australian ports that are effectively coping with disruptions across all categories of risk (see previous Figures 7-6 and 7-7). This suggestion that 30% of ports are not effectively coping in their disruption responses provides a clear conceptual signal that opportunities exist for ports to redesign and reconfigure their risk-oriented strategies, skills and processes to more effective models.

Australian port authorities must comply with their respective State legislation that requires them to develop and implement risk management plans (see DoT-WA 2018). For example, the Port of Melbourne (POM 2018, p. 4) complies with the legislative requirement by 'implementing measures and strategies… to prevent or reduce hazards and risks associated with the operation of the port' in alignment with AS/NZS ISO 31000:2018 *Risk Management Principles and Guidelines.* Port risk management systems are generally reviewed on an annual basis and incorporated into a port authority's progressive strategic development plan. Srikanth and Venkataraman (2013) argue that an effective strategic risk management process can provide the port and its stakeholders with marked competitive advantage, and

their argument resonates with the transformational and potentially unifying concepts of dynamic capabilities and business performance thinking (Teece 2007, 2017).

The survey finds that Australian ports respond in differing ways and with differing levels of effectiveness to a dynamic risk environment (Section 7.5), despite their presumed general alignment with ISO 31000:2018 risk management guidelines. From a strategic management perspective, implementation of a dynamic capabilities approach might better enable Australian port authorities to develop strategic and operational responses to an uncertain risk environment, and for them to facilitate any necessary risk management changes through internal organisational transformation and adaptation (Teece, Pisano & Shuen 1997). Further discussion on seizing this opportunity to more effectively manage port threats is taken up in the body of Chapter 8, which also contains the port resilience data analysis findings.

Chapter Eight: Resilience data analysis

8.1. Introduction

Chapter 7 reported the data analysis and findings on Australian port risk management capabilities, abilities and competencies within a dynamic risk environment. This chapter now turns to respondent opinions on port resilience, which are explored though an organisational dynamic capabilities theoretical lens. The data and literature findings are analysed to ascertain what catalysts might prompt port management to engage in transformational resilience change, what organisational strategies are employed in transforming and enhancing resilience capabilities, and to identify challenges and issues around what Teece (2018) describes as 'seizing' resilience. Chapter 8 begins by revisiting some key principals of dynamic capability theory within a port management context, as outlined in the proposed model in Figure 5-3 at Chapter 5.

8.2. Port resilience through a Dynamic Capability lens

Resilience from a dynamic capability perspective arises from transformational and reconfigured capabilities (Teece 2017a, 2018) that port managers develop and deploy to meet the unexpected, uncertain and unforeseen challenges of a changing and turbulent risk environment (WEF 2018). An analysis of Australian port managers' perspectives on organisational resilience and transformation towards strategic advantage follows a pathway that is suggested by Teece 2007) and shown in Figure 8-1. Whereas Figure 5-3 attempts to explain the relationships between dynamic capabilities and resilience theories, Figure 8-1 is a modified version that instead proposes a logic pathway for conceptualising how port resilience is managed. The value of such a resilience measurement pathway is outlined by Teece (2007, p. 1319) towards establishing clarity in how the organisation:

a) 'senses and shapes opportunities and threats;
b) seizes opportunities; and

c) maintains competitiveness through enhancing, combining, protecting, and when necessary, reconfiguring the business enterprise's intangible and tangible assets.'

Figure 8-1: A proposed model for port resilience data analysis (Adapted from Teece 2007).

The survey data analysis and findings are framed in alignment with the pathway model at Figure 8-1.

8.3. Sensing

From Teece (2007) the port's organisational dynamic capabilities towards a future resilient state begin with a process involving corporate agility and a port management capacity to understand, sense and shape opportunities and threats.

8.3.1. Resilience understandings

Thirty-six respondents viewed six alternative perceptions of port resilience (arising from the literature review) and selected one that best matched their understanding of port resilience. They were also provided opportunity to report their own preferred definition in free-form response, but this option was taken by only one respondent, marked in Table 8-1 as 'other'.

Definitions of port resilience	Responses
The port's ability to deal with both foreseeable and unforeseen risks, respond to any disruptive event, and capacity to (re)position itself for advantage after disruptions occur	36.11% (13)
The port's ability to withstand a major disruption within acceptable degradation parameters and to recover within acceptable cost and time parameters	22.22% (8)
Port management ability to maintain awareness of evolving threats, to recognise threat implications ahead of time, and to anticipate and defend against disruption before adverse consequences occur	19.44% (7)
The port's capacity to maintain safe operations when challenged by unexpected threats or hazards from all sources	11.11% (4)
The port's ability to reduce the impacts of disruptions and absorb disruptive consequences, while continuing to maintain freight throughput	5.56% (2)
A port's ability to bounce back to business as usual following a disruption	2.78% (1)
Other: Business Resilience is the development, implementation and maintenance of policies, strategies and programs to assist an organisation in preventing, preparing for, responding to, managing and recovering from the impacts of a business disruption event.	2.78% (1)
TOTAL	**36**

Table 8-1: Respondents' preferred definitions of port resilience (Author).

The first three definitions attracted three quarters of management responses, and an approximate port management understanding of resilience was derived through amalgamating definitional commonalities. These commonalities include port management abilities for mindfulness, initial response, coping and recovery. Weighting of these factors gave precedence to management abilities for coping with disruption, followed by mindfulness, in being able to recognise the onset or potential onset of disruption; organisational initial response and recovery were third placed definition factors. From this process, a composite understanding of port resilience from the respondents' preferred definitions is suggested as:

> Establishment of conditions within the port that facilitate organisational abilities for mindfulness and evaluation of potential disruptive risks, coping effectively with disruption consequences, and frequent review of strategies and processes for timely and efficient disruption responses and recoveries.

One respondent's final comments on port risk management and resilience provide a singular but interesting perspective upon the topic:

> Good risk and disruption management is not a box-ticking exercise. Resilience can only be achieved through good leadership at all levels of management (Board, administration and operational). Resilience can only take place within a well understood framework; it is difficult to measure and monitor. It is usually easier to identify a lack of good risk and disruption management through real time failures or near misses. The lack of any incidents does not necessarily indicate good risk management.

8.3.2. Analysing port resilience resources and capabilities

The Australian government (AG 2017) regards resilience as highly relevant to the security and ongoing capabilities of critical infrastructure, inclusive of ports. Within this context, thirty-one of thirty-six respondents regarded resilience as important to their port operations (86.11%), two regarded resilience as somewhat relevant (5.56%), while three (8.34%) regarded resilience as unimportant. The respondents advised what they regarded as important resources and capabilities in strengthening port resilience, as shown in Table 8-2.

The literature confirms some aspects of what port managers indicate is required in port resilience capabilities and resources:

a) understanding the risk environment and resultant port vulnerabilities (essential to the detection of potentially disruptive events – Burnard and Bhamra, 2011);
b) effective risk management planning processes (the port's capacity for response – Gallopin, 2006);
c) risk management competencies and experience (the process of strengthening resilience is reliant upon the enablement of multiple risk management options for treating diverse sources of risk – Mitchell & Harris, 2012);
d) redundancies, back-up resources and capabilities (dynamic capabilities and resources that support adaptiveness - Norris *et al.* 2008); and

e) effective governance (leading to organisational stability and sub-system stability domains – Burnard & Bhamra, 2011).

Port management opinions on port resilience components (n= 34)	
Redundancy in Port access (land/sea), communications, power in case of failure/obstructions	Understanding the key threats and having mitigation and recovery measures in place
Fit for purpose assets, master planning, recovery planning	Establishing the credible, critical issues.
Policy and procedures	Planning and training
Its ability to rapidly recover from an adverse impact or disaster	Training, up to date risk management plans and good leadership
Planning and drills/exercises	IT systems contingency plans
Having managers understand that overarching all port activities is the belief that the ports role is to manage risk appropriately.	Having redundancy in the key assets or requirements to continue vessel cargo operations
Co-operation between all companies and port towards the same goal.	Planning and attention
Management expertise and experience to mitigate disruptions where possible but also to manage post disruption in circumstances such as a cyclonic event which cannot be prevented - only planned for.	Establishing a risk management framework that ensures the organisation-wide systematic identification, assessment and management of key risks that could prevent the organisation from achieving its key objectives.
Understanding the risk	Understanding the risks and developing backup solutions in advance.
Thorough understanding of port operations and inter dependencies. Detailed engineering and site plans available remotely. Having critical spares available and a comprehensive and up to date list of resources that can be called upon at short notice	Understanding implications of "beyond the port boundary" impacts of disruption e.g. Channel closure affecting national fuel supplies
Ensure that sufficient experienced personnel are employed by the port	Flexible staff, good systems, collaboration internally and with external customers and agencies.
Preparing for events, training for events, learning from events and sharing experiences to continue to improve.	Understanding the ports business and how this fits into the needs of the State. Good BCMP plans. Good management. Good staff engagement
Having disruption plans developed, known and trained in advance	Vulnerability assessment - initial, periodic and on shift in influences. Maintenance of a Risk Register to identify known threats.
Competency and management.	Identify risks.
Workshops, formal procedures, training and drills, learn and repeat	Redundancy - resources - preparedness
Identification and management of risks/hazards	Risk assessment and management, business impact assessment, incident / emergency management, crisis management, business continuity plans, training and testing
Business continuity planning and being aware of new threats to service delivery	Pre-planning, constant reassessing, training and exercising

Table 8-2: Management perceptions of important port resilience resources and capabilities (Author).

Figure 8-2 presents port management opinions on what is required to respond more effectively to disruptive challenges. The 'sensing' requirement to understand the risk environment and vulnerabilities attracted most responses.

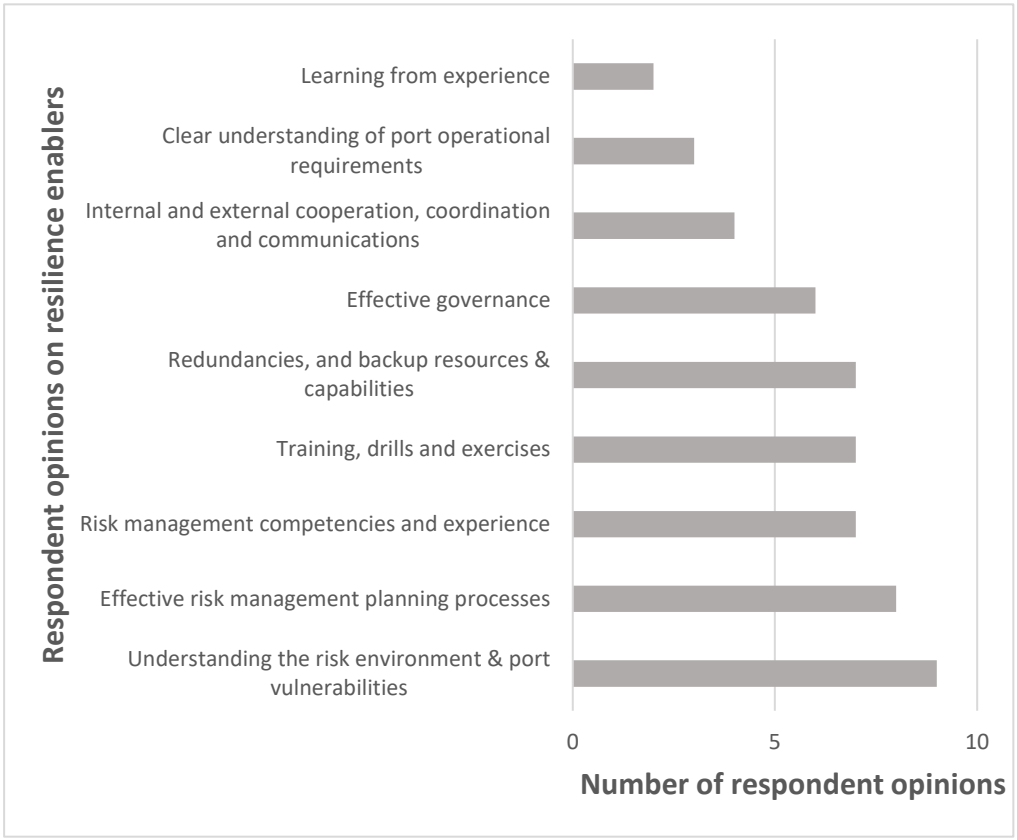


Figure 8-2: Management opinions on factors that strengthen port resilience (Author).

8.3.3. Establishing the current resilience state

Measurement of existing states of resilience appears to be a nebulous process; Coaffee and Clarke (2017) cannot find evidence of an agreed approach for measuring critical infrastructure resilience, but they do ascertain reasons why means of measurement should exist. These include being able to identify an organisation's resilience characteristics and level of capability, to identify where changes might strengthen resilience, to substantiate what resources should be allocated towards resilience, and to monitor resilience performance and effectiveness (Coaffee & Clarke 2017). Other proposed reasons include being able to demonstrate resilience progress, a need to assess leading indicators of resilience, ability to associate resilience improvements with

competitiveness, and to furnish justification for resilience expenditures (Lee, Vargo & Saville 2013).

The survey question of how to measure the port's level of resilience was answered by respondents (n = 31) who provided opinions shown in Table 8-3.

Report	Port manager suggestions for measuring current internal resilience
1	Duration of ports business returning to normal after disruption
2	Audit of emergency response capability for the most likely disruption scenarios.
3	Extended disruption times Degradation beyond expectation Complete closure of Port
4	By who's at risk due to reliance failure, board members, CEO, department head etc.
5	Number of unplanned disruptive or partially disruptive incidents. Time between incident and implementation of effective mitigating strategy and time to normal operation from incident full recovery normal operations.
6	Organisations ability to cope/recover from an event
7	A key measure will be loss of business or increased P&I insurance premiums
8	Lost revenue; Cost of incident management; Community concerns/outrage (environmental and safety)
9	Key Performance Indicators; Customer\stakeholder surveys; Board referral of high and extreme risks; Maintaining a robust risk management framework and reporting mechanism focused on key risks and treatment action plans - performing risk assessments quarterly.
10	Customer feedback
11	Unplanned downtime hours and feedback from port users during unplanned downtime
12	History
13	This can only be measured in the aftermath of a disruption. Subjective estimates can be made of gains through resilience improvements, but the nature of disruptions means that comparisons between improved and unimproved resilience are difficult or impossible.
14	Safety, productivity, customer review, financial
15	Don't know
16	Financial loss, loss of reputation.
17	Loss of revenue; risk of life
18	Poor response to minor disruptions
19	Risk management techniques
20	Not sure how one might measure the consequences of poor resilience.
21	Extended time taken to return to normal operations to meet fiscal benchmarks
22	Lengthy disaster recovery, LTI's, loss of trade
23	A little hard to quantify as it will depend upon the scenario/ nature of the disruption (be it an environmental issue, or ship/ channel blockage or a Cyber interruption)
24	Demurrage bills, reduced margin on product
25	1. Establishment of port operational and management (fiscal) metrics 2. Collection of ongoing data relating to 1 3. Desktop analysis (war-gaming) of various future paths that affect the metrics at 1 with expected outcomes on 2.
26	Time taken to re-establish operations after event; Impact on port users; Reputational damage; Financial impact (including if insurance coverage is inadequate); Regulatory breaches
27	Risk Tables using accepted consequences.
28	Interruption to services / downtime - inability to resume operations within MAO periods
29	Customer feedback; Port services outages.
30	1. Recovery time 2. Financial impact 3. Reputation impact
31	A long period of downtime after an unforeseen disruption.

Table 8-3: Respondent proposed indicators for measuring resilience (Author).

These opinions are diverse, showing that there is either lack of consensus or understanding, ranging from management 'not knowing' to submission of multiple concepts from individual managers. Management capabilities and

expertise for speaking to this issue are unknown, other than by the level of formal risk management qualifications listed in management demographics (Section 7.3). Also unknown is the extent (if any) that port managers rely on external experts for advice on the use of resilience as a beneficial operational concept.

To better understand these port management constructs of resilience, and to identify the extent of commonalities in these perceptions of resilience states, items are coded within nine themes and shown in Figure 8-3.

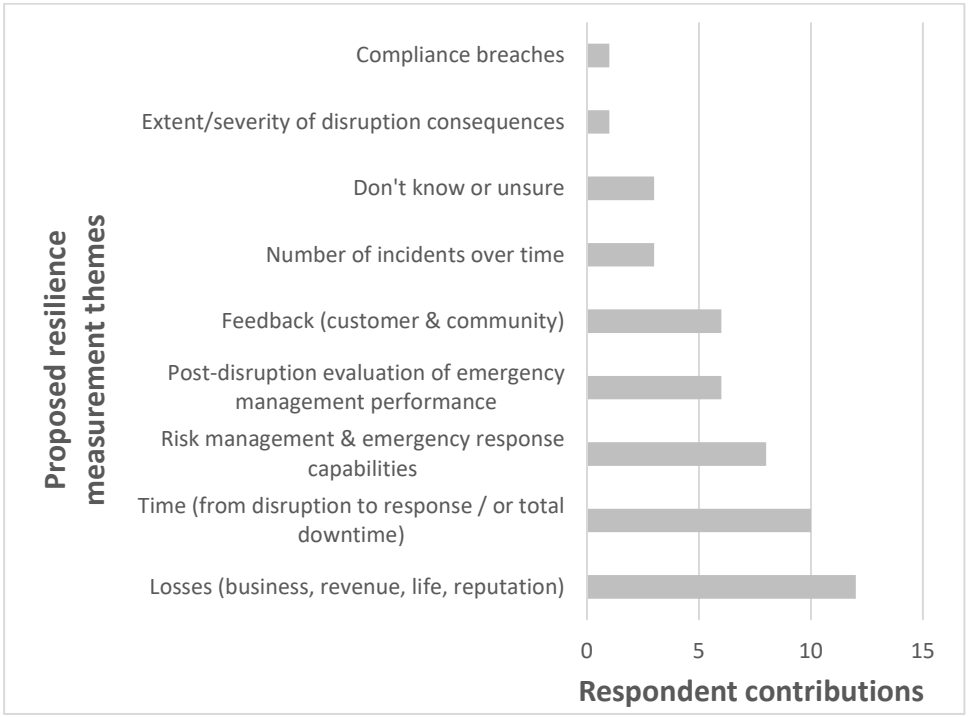


Figure 8-3: Port manager concepts of how to measure states of resilience (Author).

Responses that appear to have minimal association with resilience theory, and respondent lack of resilience knowledge suggests that much work is needed to broaden the take-up of resilience at Australian ports. For resilience to move from a minimally observed capability to a mature management capability, managers would need to construct and implement a strategic plan for progressively building port resilience (Gibson & Tarrant 2010; Bititci *et al.* 2012; Crawford, Langston & Bajracharya 2012). Performance measurement and management of resilience becomes an important practitioner concept, in providing a means for monitoring and measuring performance, control and

cost effectiveness, and in benchmarking organisational performance against desired standards and objectives (Melnyk *et al.* 2013). Figure 8-3 also indicates that the highest-ranking perceptions of resilience measurement indicators are associated with the commercial aspects of port losses and downtime. These are disruption outputs, whereas key risk management and emergency response capabilities are likely to be regarded as inputs that promote and contribute to resilience.

One respondent suggested that monitoring insurance industry risk tables might assist port managers to gain a realistic perception of their risk status from the potentially more conservative viewpoints of that port's insurer. Assessing community feedback was also suggested to gain another perspective of the port disruption management performance through either direct means (receiving written or spoken communications, or feedback access on a web site) or indirect (monitoring mainstream or social media). Monitoring social media feedback from activist organisations who either watch over port activities and report their observations on social media or take direct protest action can also be a form of monitoring for risk challenges (Marshall 2016). The final respondent indicator to be considered is that of assessing past disruption consequences for indications of whether the port's resilience level against that type of disruption has changed for better or worse, and if worse, then a need for transformational resilience change is indicated.

8.3.4. Drivers of transformational resilience change

Respondents expect fewer major disruptions in coming years (Subsection 7.5.2.). However, the literature review suggests that ports will become increasingly challenged by unknown and unpredictable adverse risks within a progressively more volatile risk environment, with higher severity natural hazards in the short-term future (Gajjar, McLeod & Wakeman 2013; Accenture 2015; Christopher & Hollweg 2017; Lam & Lassa 2017; WEF 2018). Regardless of how many disruptions port managers might experience, they will continue to be tested by changes involving new and rapidly changing technology, new sources of risk, and a need for transformation and adaptiveness if they wish to

maintain their port's business continuity (Onyeji, Bazilian & Bronk 2014; Teece, Peteraf & Leih 2016).

Normal port operations are tolerant of a certain amount of change as demonstrated by ongoing adjustments to port operations methodology following globalisation, increased security requirements post 9/11, and the impacts of technology changes, increasing ship sizes and changing markets (Burns 2015). However, at some point an increasing or sudden intensity of change may require port managers to review and strengthen their resilience capabilities. From this perspective, respondents were shown a list of twelve drivers for strengthening port resilience. These drivers were sourced from the literature, for example Coaffee and Clarke (2017). Port managers were asked to rank these drivers in order of importance from one to twelve, and results are shown in Figure 8-4. These drivers are potential incentives for motivating resilience change, and reasons why port managers might wish to outlay time, effort and budget upon resilience (Seager *et al.* 2016).

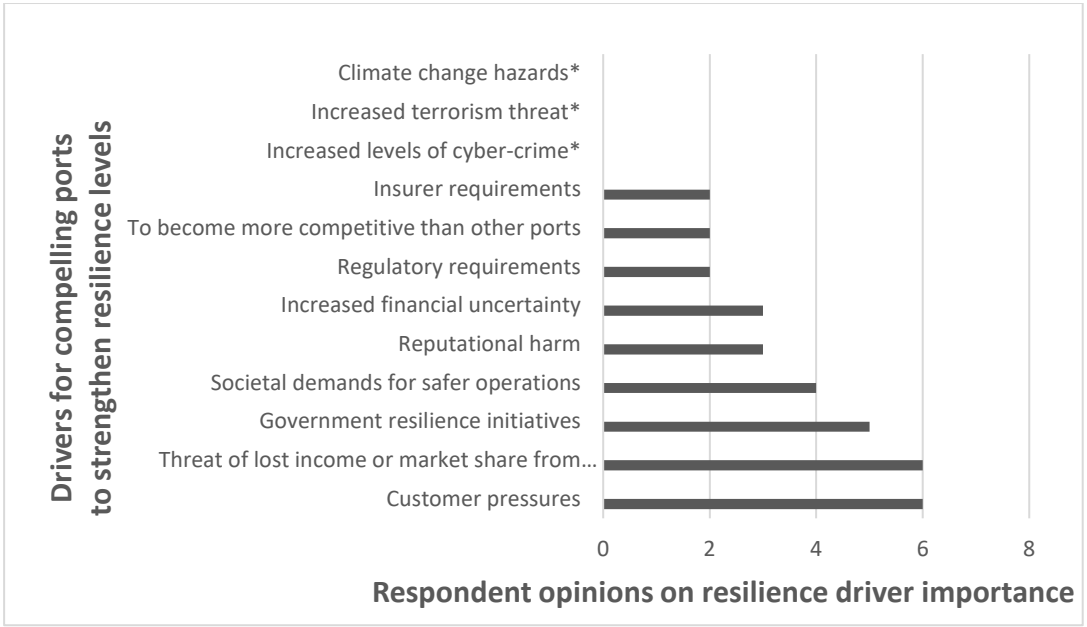


*Figure 8-4: Drivers of transformational resilience change: * represents nil consideration (Author).*

Cyber-threats and terrorism increasingly affect global transportations systems (Harris-Hogan 2017; Lawrence *et al.* 2017). The Maritime Transport and Offshore Facilities Security Act (2003) requires Australian port managers to

enhance their maritime security processes and defences. Recent ICT system breaches have been damaging and costly - the Wanna-Cry security attack alone resulted in estimated global losses of US$8 billion and the Petya virus caused estimated losses of US$850 million (Wirth 2017). Despite these influences, the findings indicate that the respondents overlook terrorism, cyber-crime and malware as important drivers towards strengthening resilience. Also overlooked are climate change hazards despite a relationship with resilience being identified by academic research (McEvoy & Mullett 2013; Yang *et al.* 2015). This finding is inconsistent with other studies that explore increased levels of resilience towards mitigating the consequences of climate change (for example, Becker *et al.* 2015; Chhetri *et al*. 2015; McEvoy & Mullett 2015). Also, because port managers acknowledged earlier in the survey the growing likelihood of increasingly severe natural events (Subsection 7.5.2), then their rationale for ranking climate change as an unimportant driver for resilience enhancement remains unclear.

Motivation for resilience change and reconfiguration might arise as senior managers become increasingly involved with the Australian government's Trusted Information Sharing Network (TISN) critical infrastructure working groups and committees (TISN 2016). Much of Australian critical infrastructure is privately owned and operated, and the national government promotes private sector critical infrastructure resilience 'by encouraging a business model that incorporates a focus on organisational resilience' (O'Donnell 2013, p. 25). However, port authorities while deeply involved with commerce are not part of the private sector. They are corporatised government business agencies with limited autonomy, and their State government owners have potential to prevail over port 'managerial and decision-making autonomy' (Brooks, Cullinane & Pallis 2017, p. 6). This suggests that if State governments wish their ports to increase resilience levels, then this might be achieved either by formal regulatory directions, or informal measures taken by the relevant Ministers to encourage transformational change.

The findings on drivers of transformational resilience change suggest that Australian government work in promoting critical infrastructure resilience is making inroads. Respondents rate government resilient initiatives as their third highest motivating factor.

8.3.5. Transformational resilience learning practices

Respondents acknowledged the role of learning in strengthening port resilience. A common perception is that learning from experience, coupled with training, drills and exercises are important foundations for sensing the need for change and maintaining preparedness against the risk environment. The literature provides evidence that systemic complexity and multiple sources of vulnerability lends importance to port risk managers developing analytic risk management, collaboration and communication skills of a high order (Pallis & Kladaki 2016). In this context, the role of education appears to be increasingly important for port managers' analyses of the risk environment and port vulnerabilities to risk (Hopkin 2017). According to Kayes (2015) learning from experience is a key organisational resilience enabler, and in the absence of ongoing formal and experiential learnings, the organisation becomes more vulnerable. Figure 8-1 (resilience pathways) shows a return loop from 'managing threats' back to the 'sensing' and monitoring phase of managing resilience.

8.4. Seizing opportunities from transformational resilience change

Following the identification and analytic processes involved in assessing internal and external threat (sensing), according to Teece (2017b) the dynamic capabilities model next addresses how resources, assets and capabilities might be deployed to best address these threats and to capture value if possible within transformational change (seizing). From an organisational resilience context, the seizing process entails the use of concepts, resources and assets that senior management deems to be most suited and likely to achieve success (Teece 2017b). Senior management commitment towards transformational change and building resilience are potentially driven most in the presence of major threats to their organisation (Teece 2017b).

8.4.1. Management support for port resilience

Management leadership and advocacy for port resilience are crucial factors in enhancing organisational resilience (Southwick *et al.* 2017). Managers were asked their opinions on what aspects of resilience support were important to their organisations. These factors were adapted from the literature, including Stephenson (2010), Fiksel (2015) and AG (2016). Responses to questions (n=36) related to management inputs to resilience are shown in Table 8-4. Most respondents treated all factors involving management support of resilience concepts as important.

Management support of resilience	Important	Unimportant	Neutral/unsure
Encouraging greater initiative and flexibility	35	1	0
Empowering decision-making based on incomplete information	34	2	0
Empowering improvised solutions	35	0	1
Constructive performance reviews and feedback	35	1	0
External collaboration	34	1	1
Inter-organisational resource sharing	34	0	2
Collaboration with emergency response agencies	35	0	1
Transparent and available succession management plans	32	4	0
Discouraging management and data silos	30	4	2
Deferment to expertise and experience over rank	29	4	3
Understanding of what core operational objectives enable business continuity	34	1	1
Regular management briefings on the risk environment	32	3	1

Table 8-4: Resilience support and leadership (Author).

Two heads of department and two Harbourmasters regarded as unimportant the concept of relaxing managerial control over availability of succession management plans, the deferment of expertise and experience over rank, and discouragement of management and data silos. Additionally, two managers (Harbourmaster and head of department) were unsure about the value of discouraging silo management, while three managers (CEO, Harbourmaster and head of department) were uncertain about deferment to expertise over rank during disruptive circumstances.

8.4.2. Factors in building resilience

Respondents were asked for their opinions on what management initiatives were crucial in building resilience at Australian ports, based on a list compiled

from the literature review. The composite responses are shown in Figure 8-5. The respondents (*n* = 33) demonstrated a high level of agreement for these initiatives, and most respondents recognised the value of senior management support for resilience management programs.

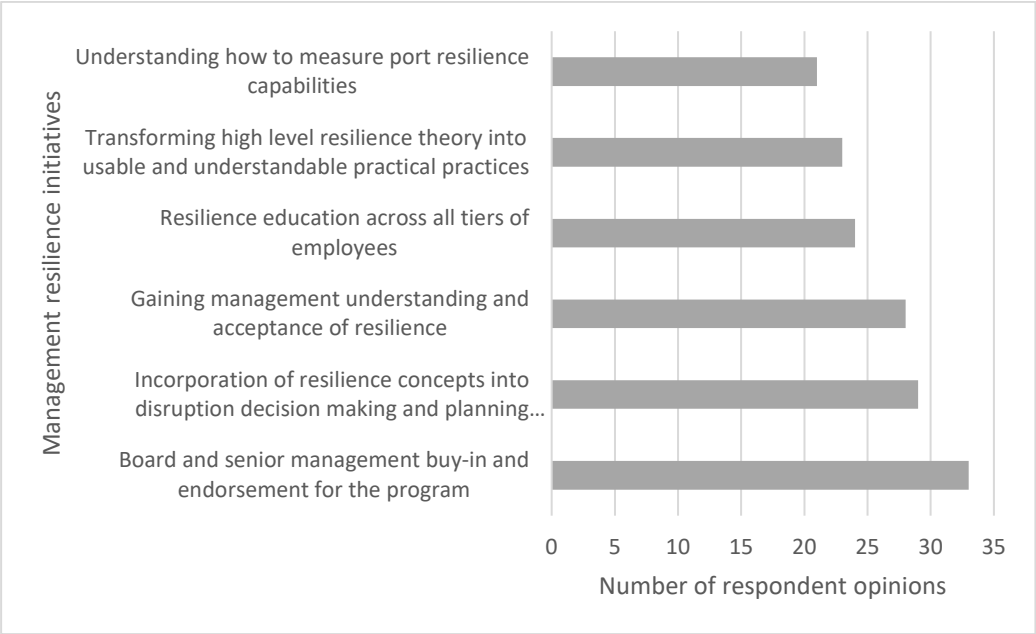


Figure 8-5: Factors for building port resilience (Author).

Opportunity was provided for free-form responses with respondents being asked what other management initiatives or factors might be crucial to increasing port resilience levels. Free-form replies included:

a) 'Inculcation of initiative and problem-solving (as distinct from problem-identifying) across and throughout the organisation'; and
b) 'Sufficient experienced and flexible personnel'.

These two responses align with resilience governance principles that are at the heart of socio-ecological system resilience. Berkes (2017) argues that resilience and adaptive behaviour benefit from a collaborative approach across the whole system, whereby personnel at all levels have opportunity to contribute to disruption response and employ their knowledge and skills to organisational benefit. Empowerment of staff initiative and problem-solving at an individual level is therefore important in employee engagement and decision-making. Having sufficient experienced and flexible personnel across the organisation capable of making these contributions is equally important.

8.4.3. Aids and impediments to change

Everett (2003a) and Pettitt (2014) describe Australian port authorities as conservative and bureaucratic in outlook, with these restraining influences flowing over into port performance efficiencies. Q28 investigates Australian port managers (*n* = 36) mindsets towards acceptance or rejections of operational resilience concepts, and finds (Figure 8-6) that conceptually, respondents are generally in favour of embracing resilience concepts, but when commercial implications are considered then fewer are in favour (16 agree; 16 disagree).

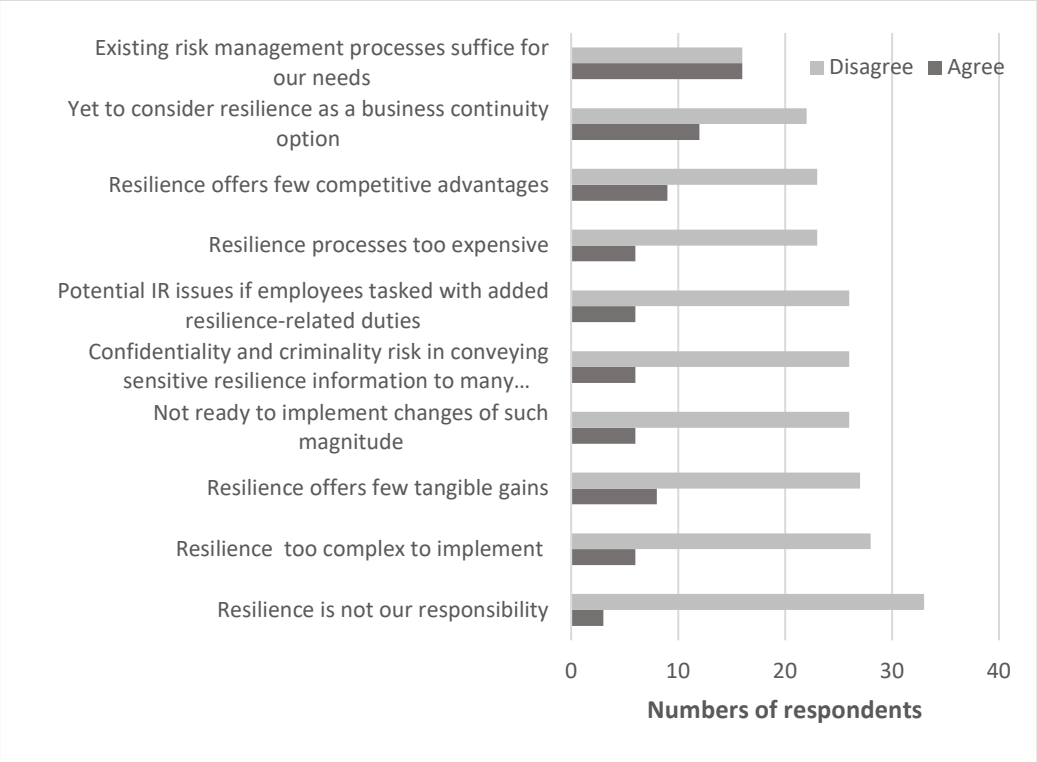


Figure 8-6: Attitudes to resilience change (Author).

The data reveals that half of the respondents to this question were not intending to change from their conventional risk management practises and processes, and they perceive a range of limitations against them adopting resilience concepts and capabilities within their port organisation. In advising whether their existing risk management systems sufficed, respondents were effectively crystallising their acceptance or non-acceptance of resilience. If resilience is primarily perceived as a conceptual topic, then managers appear to be accepting of resilience concepts. However, when the practical processes

and consequences of implementation (or lack of tangible benefits to the port) become considered and evaluated within open-ended responses, then resilience is viewed less favourably. Impediments include increased costs, minimal perceptions of competitive or business continuity advantages, and belief that existing risk management system/s suffice. As discussed in more detail within the conclusions chapter, these findings provide evidence that a stronger catalyst for resilience change is needed for Australian government critical infrastructure resilience initiatives to take further hold in national ports.

Respondents provided qualitative information on impediments to increasing port resilience, including socio-political influences and constraints (Subsection 8.4.3.). Examples provided by respondents include tighter government controls over port expenditures as governments increase port dividend payments as part of balancing State budgets. Other impediments are primarily related to commercial considerations, including increased costs, minimal perceptions of competitive or business continuity advantages, and beliefs that existing risk management system/s suffice in lieu of change.

8.5. Managing threats – resilience transformation

Teece (2017b) argues that a transformation process may require the organisation to selectively change its operating models, methods, culture and its lines of communication. Integral to this process is recognition of what existing capabilities, practices and resources are relevant to emerging transformational resilience strategies, and what additional capabilities are needed (Teece 2017a). The gathered data provides evidence of existing port management resilience understandings, beliefs, and capabilities.

8.5.1. Resilience governance

In response to Q26, 91.67% of senior managers soundly recognise the importance of Board and senior management buy-in and endorsement for a resilience program. Their perspectives of resilience governance extend to agreement that managers should be permitted to exercise an extended degree of initiative, flexibility, improvisation and decision-making made in their

disruption management responses (Q23 responses). There was no mention in the 'additional comments' section of the survey in relation to the degree of autonomy that managers at differing levels might be permitted to exercise during emergency management and business continuity response events.

8.5.2. Aligning existing capabilities

Data analysed within the port risk management reports furnishes evidence that existing capabilities for managing threats are of variable performance levels, and particularly so for the more intangible or covert causalities (for example cyber-threat). These findings group existing capabilities in four levels of port risk management outcomes, where port managers:

e) respond, manage and recover from disruptions;
f) respond, manage and recover from disruptions, but with difficulties;
g) respond, manage and recover from disruptions, with external assistance; or,
h) are unsure whether they can respond, manage and recover from these categories of disruption.

These findings suggest that gaps exist in Australian port abilities to cope with high consequence disruptions carrying potential to close ports, and that where these gaps exist, transformational resilience change would be beneficial.

8.5.3. Resilience resources

Respondents also note a need for change in improving internal and external communications, collaboration and preplanning with external agencies. This is to assist when the disruption recovery process requires external assistance. A requirement for external assistance is associated with either accessing extra resources as with the case of an oil spill, or for regional emergency responders. One respondent noted that a complete disruption management capability involves: 'reliance on emergency response agencies (i.e. Police, Fire)'. In such a case the port might initially barely cope or be unable to cope without this external assistance. Another respondent noted quality issues in disruption management when personnel are recruited through outsourced recruiting

agencies, and managers are unsure of what emergency skills these personnel possess. Two respondents reported that they were unsure of how well their organisation managed to cope with disruptions of human causality, which may relate to a requirement for a benchmark study.

Respondent opinions of necessary changes in port practices to improve resilience (Subsections 8.3.4.; 8.3.5.) include the development of flexibility, adaptiveness, and disruption preparedness. First physical component priority is enablement of backup generators; oil/chemical spill response items; firefighting equipment; command, control and communications systems and stores; and, ICT system backup batteries. Essential supplies are next listed priority, with requirements for onsite water and fuel reserves, and rescue/medical items and equipment. Third priority is for trailer mounted tower lights for emergency illumination. Surprisingly, minor priority is afforded to offsite or cloud data backup of data, applications and services, which might otherwise be construed as an essential component of disruption recovery strategy (Langer 2017).

8.5.4. Gaps in port resilience capabilities and competencies

Where resilience exists in Australian ports, then intuitively it is most likely to exist within the ports that most capably manage disruptions. However, the evidence gathered in this research provides mixed evidence of port resilience mindsets and intentions. Whereas port managers can be assessed for their levels of risk management understandings, experience, qualifications and capabilities, difficulty arises in identifying the extent of their resilience capabilities and competencies. Brodsky *et al.* (2011) describe resilience behaviour as 'superior performance' but from a research perspective there is little within the literature to enable measurement of resilience capabilities and capacities, rather, researchers are more likely to ascertain whether organisational culture and conditions are favourable or otherwise for encouraging resilience-oriented behaviour and mindsets.

The data shows that thirty-one of thirty-six respondents regard resilience as important to their port operations (86.11%) and are generally in favour of

embracing resilience concepts (Subsection 8.4.1.). Nonetheless, half of the survey respondents are not intending to amend their conventional risk management practises and processes by adopting resilience concepts and capabilities (Subsection 8.4.3.). Respondents consider that the strongest likely influences for change and for them to strengthen their levels of resilience are;

a) customer and societal pressures for higher levels of resilience;
b) if non-compliance with resilience concepts resulted in their port losing income or business; and/or
c) macro-government initiatives require them to comply with resilience legislation or guidelines (Subsection 8.4.2.).

Eighty six percent of managers regard resilience as important to their organisation (Subsection 8.4.1.) however, a need for mindset change becomes apparent when resilience becomes considered within a commercial context, and managers react negatively to the likely costs and effort involved (Subsection 8.4.3.). Data results show that respondents become less disposed towards resilience implementation when commercial ramifications are considered.

Despite a body of research that identifies cyber-threats, terrorism and extremism as major future threats to global transportation systems (Harris-Hogan 2017; Lawrence *et al.* 2017), these hazards were ignored by the survey respondents as drivers for strengthening port resilience (Subsection 8.3.4.). Also overlooked are the risks of climate change hazards, despite well-established relationships between climate change, extreme weather events, and the importance of resilience capabilities within academic and business research (Downing, Olsthoorn & Tol 2002; McEvoy & Mullett 2013; Yang *et al.* 2015; Ng *et al.* 2016; Henderson *et al.* 2017).

Respondents also note a need for change in improving internal and external communications, collaboration and preplanning with external agencies. This is to assist when the disruption recovery process requires external assistance. A requirement for external assistance is associated with either accessing extra

resources as with the case of an oil spill, or for regional emergency responders. One respondent noted that a complete disruption management capability involves: 'reliance on emergency response agencies (i.e. Police, Fire)'. In such a case the port might initially barely cope or be unable to cope without this external assistance. Another respondent noted quality issues in disruption management when personnel are recruited through outsourced recruiting agencies, and managers are unsure of what emergency skills these personnel possess. Two respondents reported that they were unsure of how well their organisation managed to cope with disruptions of human causality, which may relate to a requirement for a benchmark study.

Respondent opinions of necessary changes in port practices to improve resilience (Subsection 8.3.4.; Subsection 8.4.2.; Subsection 8.4.3.) include the development of flexibility, adaptiveness, and disruption preparedness. First physical component priority is enablement of backup generators; oil/chemical spill response items; firefighting equipment; command, control and communications systems and stores; and, ICT system backup batteries. Essential supplies are next listed priority, with requirements for onsite water and fuel reserves, and rescue/medical items and equipment. Third priority is for trailer mounted tower lights for emergency illumination. Surprisingly, minor priority is afforded to offsite or cloud data backup of data, applications and services, which might otherwise be construed as an essential component of disruption recovery strategy (Langer 2017).

8.6. Summary

From a dynamic capabilities perspective, Australian port resilience appears to be at an immature stage of implementation. In general, the port managers indicate that their existing capabilities and competencies for managing threats are not coping well. Prior to aligning existing organisational risk and vulnerability management practices with resilience concepts, the data indicates that in general, Australian port risk management foundational resources, practices and knowledge should be improved before any resilience configuration takes place. The data also indicates a reluctance by port

managers to adopt resilience concepts in preference to their existing risk management practices.

For resilience to be operationalised either as port managers understand the concept, or in another form, the hardest hurdle to overcome appears to be changing port management culture. Australian port authorities have been described as conservative and bureaucratic in outlook (Everett 2003a; Pettitt 2014), and possibly these restraining influences contribute towards a reluctance for change. The research indicates that port motivation to operationalise resilience is most likely to eventuate from the endorsement and advocacy of Board and senior port executives. The survey found that other potential resilience enablers include:

a. commercial dictates,
b. political promotion and imperatives,
c. potential for reputational harm, and
d. regulatory compulsion to enhance critical infrastructure resilience capabilities.

The following Chapter 9 recapitulates the research problem, presents the research conclusions, and recapitulates the importance of these findings to port risk and resilience management knowledge.

Chapter 9: Conclusions

9.1. Introduction

This study set out to determine how Australian ports might manage a changing risk environment that brings new and unexpected categories of hazards, and increasingly severe natural hazards. A further objective was to assess how resilience might be operationalised within an Australian port risk management setting. The research addresses a difficult and complex topic, and endeavours to provide clearer understandings to knowledge areas for which the literature is incomplete. This final chapter summarises the most important research findings and potential value to the knowledge, and other findings are summarised at each chapter. Potential limitations of the study are outlined and discussed in terms of the findings application and generalisation to the wider port population and other transportation settings. Implications of the study for current theory and the development of future research are proposed. The research findings are summarised firstly within a literature review context, and then the empirical study findings are presented. The chapter begins with a reiteration of the study purpose.

9.2. Managing port risks

The study title 'Safe ports for the 21st Century: Australian port resilience' relates to the purpose and operational workings of a port, which enable a ship to approach, enter, use and depart the port without undue incident (Chong 1992; Girvin 2017). This thesis explores and assesses the underlying risk management concepts, practices and business continuity measures that contribute to the port's intermodal effectiveness and efficiencies. To gain this understanding, the literature review and empiric research address the following research questions:

> PRQ: How does the port manage risks and consequences arising from low probability/high consequence disruptions?
>
> SRQ1: How do ports currently manage risks and unknown unknowns arising from disruptive events?
>
> SRQ2: What do ports need to change in their practices to become more resilient? and

SRQ3: How might ports operationalise resilience to best manage/overcome risks and unknown unknowns arising from disruptive events?

The research findings suggest in general that a desirable operational state for ports to achieve is one in which managers minimise the port's exposure and vulnerabilities to new and existing hazards, and in parallel, optimise the port's capabilities and capacities to anticipate, respond to, and recover from the impacts and consequences of these hazards (Aitsi-Selmi *et al*. 2015).

9.3. Addressing the research questions

The primary research question leads to an investigation of how Australian ports manage risks and consequences arising from low probability/high consequence disruptions. This thesis investigated the primary research question from a narrow intermodal business continuity focus, while acknowledging that port managers have a broader mandate to manage risks and safety to avoid injuries and death, protect the environment, to avoid or minimise financial loss, and maintain the port's reputation for sound corporate governance. Effectiveness in one area of risk might reduce effectiveness in another - for example increased operational effectiveness leading to higher productivity might arguably expose the port to larger potential for environmental risks.

Despite a comprehensive investigation of the literature, the researcher found no evidence of any criterion that indicates what constitutes an acceptable level of risk management effectiveness for Australian ports. As discussed in Chapter 4, port decision-making concerning what levels of risk management effectiveness should be attained, and in what areas of port activities, is largely a matter for individual port risk governance strategies and policies, coupled with the influences of internal/external auditing and regulatory compliance oversight. The investigation sought answers to the research questions from the port-centric risk and resilience literature, which then informed the empirical research. Conclusions from these two major phases of the investigation are shown in the following sections.

9.4. Findings from the literature

Australian ports are highly valuable critical infrastructure whose characteristics have transformed over the years into regionalised complex systems of interrelated and interdependent logistics, resource and transportation actors. Ports are recognised by the Australian government as vital to national trade, economic well-being and national prosperity (NTC 2011). However, the extended nature of the port's own supply chain and support organisation renders it increasingly vulnerable to disruptions that might either impact the port directly, or through the consequences of failure involving second or third parties of critical importance to port operations.

Critical areas of vulnerability arise where port intermodal operations rely upon tangible and intangible port management resources (Madani 2018), its physical attributes and infrastructure (Trujillo & Nombela 1999; Hsieh, Tai & Lee 2014; Black *et al*. 2018), human capital and management systems (Rose, Wei & Paul 2017; Madani 2018), and, its technological support (Paté-Cornell *et al.* 2018). The literature shows that port vulnerabilities alter over time, which means that port risk management processes and procedures should also undergo review and modification. Ports are dynamic critical infrastructure whose characteristics undergo multiple planned and unplanned transformational changes arising from changes in ship size and designs, new cargo types and handling methods, globalisation, port privatisation, growth in trade volumes, the rapid pace of technology change, expansion in the number of industry participants and resulting complexity, plus competition with other ports.

The comprehensive literature review finds few examples of research, theory and guidance of direct relevance to Australian port vulnerabilities to their risk environment, and consequent emergency management capabilities. One study (Rice & Trepte 2012) examines US port resilience within the context of management's abilities to react to and manage unexpected disruptions, and to effectively and efficiently restore normal port intermodal operations. They found that while the studied ports might demonstrate resilience to minor day-to-day incidents, the port resilience effectiveness deteriorates against major disruptions.

Their approach aligns with that of this thesis, and one of their general findings was that the surveyed US port managers had little understanding, interest or regard for the concept of port resilience. Little evidence is found of US port managers consciously incorporating resilience concepts within their disruption management strategies and decision-making protocols. They also find that multiple US port managers and port stakeholders are insufficiently prepared to cope with high consequence disruptions, particularly if major damage results to infrastructure and superstructure. Their recommendations for how to build resilience include increased capital expenditure to provide redundancies in these physical aspects of port intermodal operations, and conceptually, for a greater resilience focus on port business continuity plans. Resilience growth is argued to be impeded by the perceived fragmentation and lack of coordination between port-centric stakeholder networks and their freight task activities. Port resilience levels can be increased, according to the Rice and Trepte (2012) study, following improved integration, collaboration and communication across the breadth of port stakeholder networks. Rice and Trepte (2012) conclude that their studied ports are resilient but not resilient enough, and port managers need to improve their resilience focus and competencies. Their findings confirm those of this thesis.

9.4.1. Port management competencies

The literature suggests that effective port risk managers require an understanding of increasingly complex concepts and terminology, analysis processes and knowledgeable risk management leadership. Contemporary risk governance towards complex risks, according to De Marchi (2015, p. 162) requires managers and academics to recognise that such complexities exist, and to realise that risk complexities can be neither 'be fully understood nor managed with traditional risk assessment tools'. Decision-maker competencies to understand advanced risk management tools may be needed soon, because increasingly, Australian port managers conduct their operations within dynamic and complex operating environments, with vulnerability sensitivities to diverse risks both within their ports, and within their external networks of crucial goods and services providers. Port management preparedness to meet these systemic complexity challenges

requires strong and informed risk management leadership (Hellingrath *et al*. 2015).

9.4.2. Port risks and vulnerabilities

The literature shows that the Australian port risk environment is shaped by three categories of risk (Robinson, Francis & Hurley 2013; Hopkin 2017):

a) hazards with negative consequences (pure risks);
b) uncertainties and unknowns (control risks); and,
c) legislative, regulatory or code of practice requirements for hazard management (compliance risks).

The literature findings in Chapter 4 show that external risks require organisational mindfulness for early recognition, preparedness to respond, and capabilities for minimising and recovering from the risk consequences. Alternatively, organisational compliance risks are largely avoidable through establishing complying systems and conditions, and monitoring and guiding personnel behaviour. Risks involving uncertainties and unknowns require preparedness in the form of encouraging an adaptive and innovative mindset and generic response capabilities and resources. The literature also informs practitioners of emerging new millennium risks (WEF 2018), some of which have potential to substantially affect the conduct of Australian port operations. These are external risks whose causalities are beyond port management abilities to control. The World Economic Forum (WEF 2018, p. 3) presents its expected ten most likely millennium risks for the short term, as shown in Table 9-1.

Economic	Environmental	Geopolitical	Societal	Technological
Illicit trade	Extreme weather events	Terrorist attacks	Large-scale involuntary migration	Cyberattacks
Economic crisis	Natural disasters			Data fraud or theft
	Man-made environmental disasters			
	Failure of climate-change mitigation and adaptation			

Table 9-1: Top ten most likely risks to global institutions (Adapted from WEF 2018).

The thesis survey established that Australian port managers are mindful of these risk types, and port managers reported already experiencing adverse consequences from some disruption types and provide their expectations for future occurrences. In meeting diverse risk types and categories, port risk governance systems must encompass strategic and tactical planning, decision-making, and risk treatments aligned with the objective of achieving strategic and operational objectives (Lark 2015; ISO 31000:2018). Within this thesis, whereas survey respondents appear to be aware of differing risk categories at an abstract level, they provide little evidence of modifying their risk management processes to treat differing risk categories with separate methodologies or higher-level capabilities.

Port managers must manage vulnerabilities related to the risks of routine failures, human error, cyber-attack, physical security, rapid advances in technology, the vagaries of weather, and the integrity of their electrical supplies (Section 2.3.). Typically, Australian port authority risk and vulnerability identification takes place within annual brainstorming sessions (Srikanth & Venkataraman 2013). The literature review suggests a potential new direction and a more structured approach to how port managers perform their risk identification and vulnerability assessments, by use of a military technique (Schnaubelt, Larson & Boyer 2014). This technique takes the preliminary step of conducting vulnerability identification and assessment, rather than first identifying a hazard and then assessing how the port might be vulnerable. This technique provides a defence-in-depth evaluation of operational susceptibilities by ranking port weaknesses and vulnerabilities in order of:

a) critical capabilities essential to achieving port logistical and transportation objectives;
b) critical requirements in support of critical capabilities, in terms of management, assets and infrastructure resources coupled with relevant knowledge, plans, policies and strategies; and
c) critical vulnerabilities - whereby critical requirements, or second party contributors to these requirements, are insufficiently prepared or assessed

as being incapable of responding to or managing disruptions and their consequences.

9.4.3. Australian port risk management

Port risk management and governance characteristics vary from port to port in complex multiple aspects, driven by differing port needs and interests, and varying elements of uncertainty and complexity associated with whichever risks affect each port (De Marchi 2015). Australian port managers have access to a diverse range of guides, techniques and approaches to assist them in developing their risk management capabilities and capacities as outlined in Chapter 4. Their primary guide is the ISO 31000:2018 *Risk management -- Guidelines* standard, which the Australian State government port owners advocate for port management use. Port managers might have difficulty in absorbing and making sense of the many documents that comprise the risk management and resilience standard families, and which narrowly address specific aspects of risk, resilience and business continuity.

The researcher adapted from literature sources a port risk management maturity model to assist in better understanding the progressive path of port risk management effectiveness. The proposed risk management maturity model as explained in Section 4-8 is presented for convenience in Figure 9-1. The model combines the features of other models (Chapman 2011; Andrews 2017; Kolomiyets 2017) with the addition of a percentage effectiveness scale on the y-axis to provide an ability for quantification. The model is also constructed to show how conventional enterprise risk management processes and procedures form the basis for port resilience, which indicates that preceding levels of risk management capability should be attained before resilience becomes fully effective. Based on the empirical findings, Australian port capabilities appear for the most part to fit within the level four column, in which risk management expertise and competencies are categorised as established and consistent.

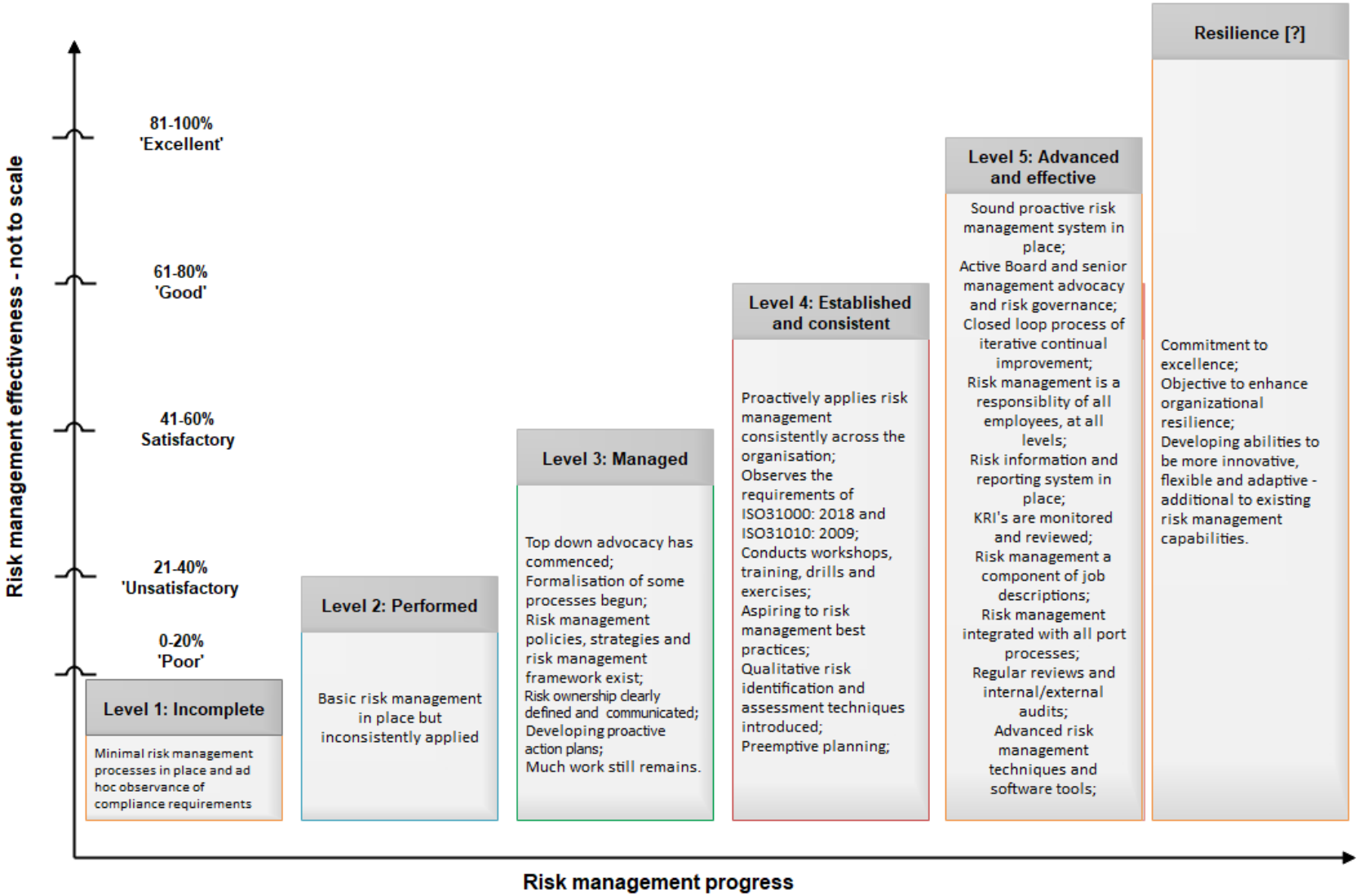


Figure 9-1: Characteristics of a port risk management maturity model (Adapted from Chapman 2011; Andrews 2017; Kolomiyets 2017).

9.4.4. Higher level risk management

Conventional risk management strategies and techniques, practised for many years, enable port managers to directly prepare for and treat known hazards and associated risks (Blades 2017). For unknown risks and hazards, port managers require generic risk management solutions to cope with unpredictable risks, and these solutions might be strengthened with acquired abilities for adaptive, innovative and improvisational responses at all levels of management. The literature advises that additional and enhanced risk management capabilities involve the design and incorporation of resilience frameworks and models into port management practices. This evolution towards higher level risk management better prepares port managers for responding to unknown, unanticipated, and otherwise unmanageable new and emerging risks (Linkov *et al.* 2014; WEF 2018).

Resilience frameworks as described in *ISO 22316:2017, Security and resilience - Organizational resilience - Principles and Attributes* necessarily differ between organisations, with specific objectives and initiatives incorporated within each framework to suit individual organisational needs. The major components of a resilience framework as outlined within the resilience standard and elsewhere I the literature include an identification and understanding of the organisation, an analysis of current capabilities and vulnerabilities, setting objective and requirements, identification of internal and external resources and stakeholder dependencies, and formulating the strategies and methodologies for implementing and enhancing resilience capacities (Linkov *et al.* 2014; Häring *et al.* 2017; ISO 22316:2017). Multiple examples of resilience frameworks were found in the literature from both social-ecological and engineering resilience approaches, including those just cited, however there was minimal evidence of a generic port resilience framework that provides a non-complex overview of how higher levels of port resilience might be engendered.

The researcher developed from the resilience literature sources (for example ISO 22316:2017) a resilience management framework to assist academics and port managers in better understanding the stages involved in the evolution, implementation and maintenance of these resilience management practices in a

port context. The proposed framework (as explained in S 5-5) is presented for convenience in Figure 9-2, as a pragmatic blueprint overview of how resilience concepts are transformed into port practice. The framework aims to advance port resilience knowledge but leaves processual gaps in understanding what each step entails. The thesis accordingly turned to the literature for a model that explains in more detail how ports might operationalise resilience.

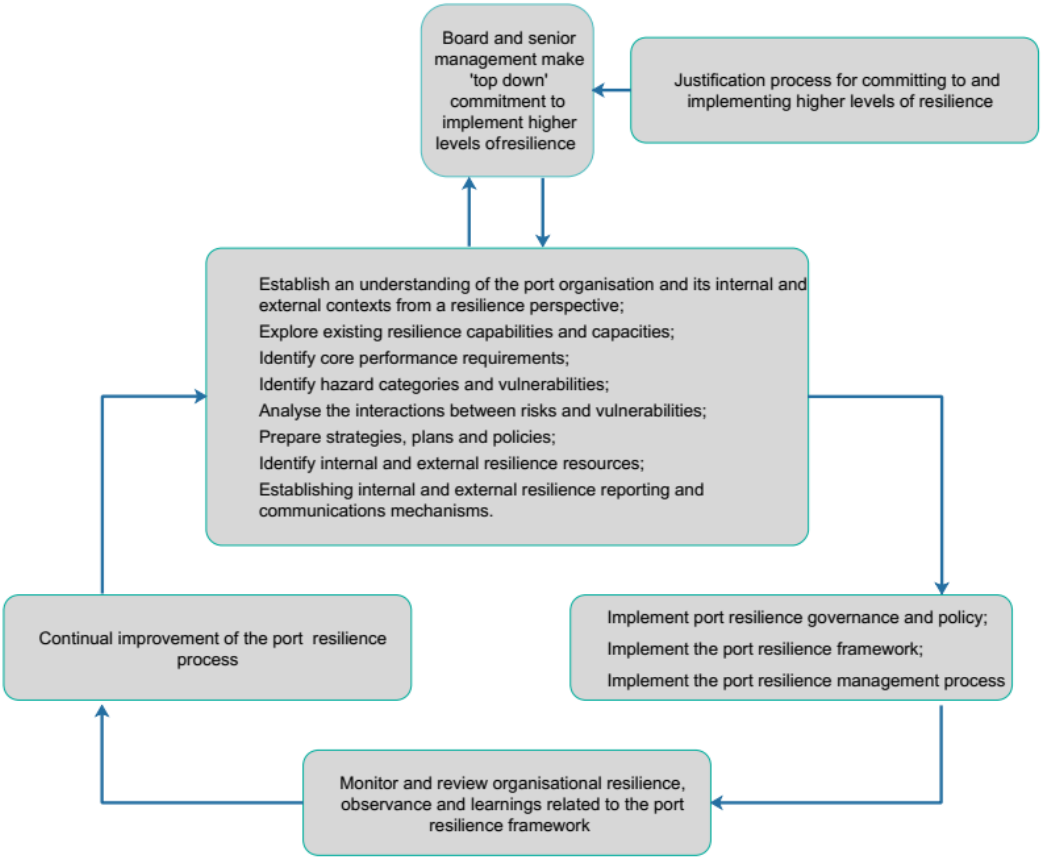


Figure 9-2: Conceptual port resilience implementation framework (Adapted from ISO 22316:2017 concepts).

9.4.4.1. Understanding how to operationalise port resilience

The research set out to establish how resilience might be operationalised at Australian ports and the inherent challenge with this task is that resilience is regarded as a port management intangible resource (Hall 1993) and as such is not directly detectable or measurable. Rather, proxy indicators (Brown, Seville & Vargo 2017) are used to detect organisational preparedness to implement resilient responses to either day-to-day emergencies or major crises (McManus *et al.* 2008). McManus *et al.* (2008, p. 81) argue that enablement of resilience

requires ‘situation awareness, management of keystone vulnerabilities, and adaptive capacity.’ Consequently, if resilience is an intangible resource that cannot be seen or measured, then how can it be operationalised, analysed, documented and aligned with existing risk management capabilities? Whereas the literature provides some answers regarding what organisational resilience and its values to the organisation might be, there is less evidence from a business model perspective of how an organisation might operationalise resilience at the required level, what motivates it to do so, how existing resources and capabilities are realigned, and what new capabilities are needed. To narrow this evidence gap, the researcher explored organisational theories for a suitable model to explain how managerial risk management cognition and abilities might transform towards a functional and cultural resilience capabilities mindset.

This type of problem solution resonates with the dynamic capabilities concepts of value creation and capture (Teece 2017). Dynamic capabilities theory particularly lends itself to studies involving middle management’s bottom-up innovation in transforming new knowledge or methodology into regular use (Teece 2018) which in this thesis refers to operationalising resilience concepts. Dynamic capabilities theory (Teece, Pisano & Shuen 1997) was found in the literature survey to have much in common with resilience concepts (for example, flexibility, complexity, innovation, adaptiveness, improvisation, transformation, learning, coping with threats and sudden change, managing uncertainty, systemic change, situational awareness, dynamic processes, governance and leadership (Teece, Pisano & Shuen 1997; Teece 2007; Teece 2017; Teece 2018). A port organisational resilience dynamic capabilities model was developed from the literature, to assist in understanding how port resilience might be operationalised, and to identify where empirical investigation is needed to address gaps within the knowledge. The proposed model as explained in Section 5-2 is presented for convenience in Figure 9-3 as part of the literature findings, and then its individual components are examined and aligned with the empirical research findings in Section 9.6, to provide a method for operationalising resilience within port management practices.

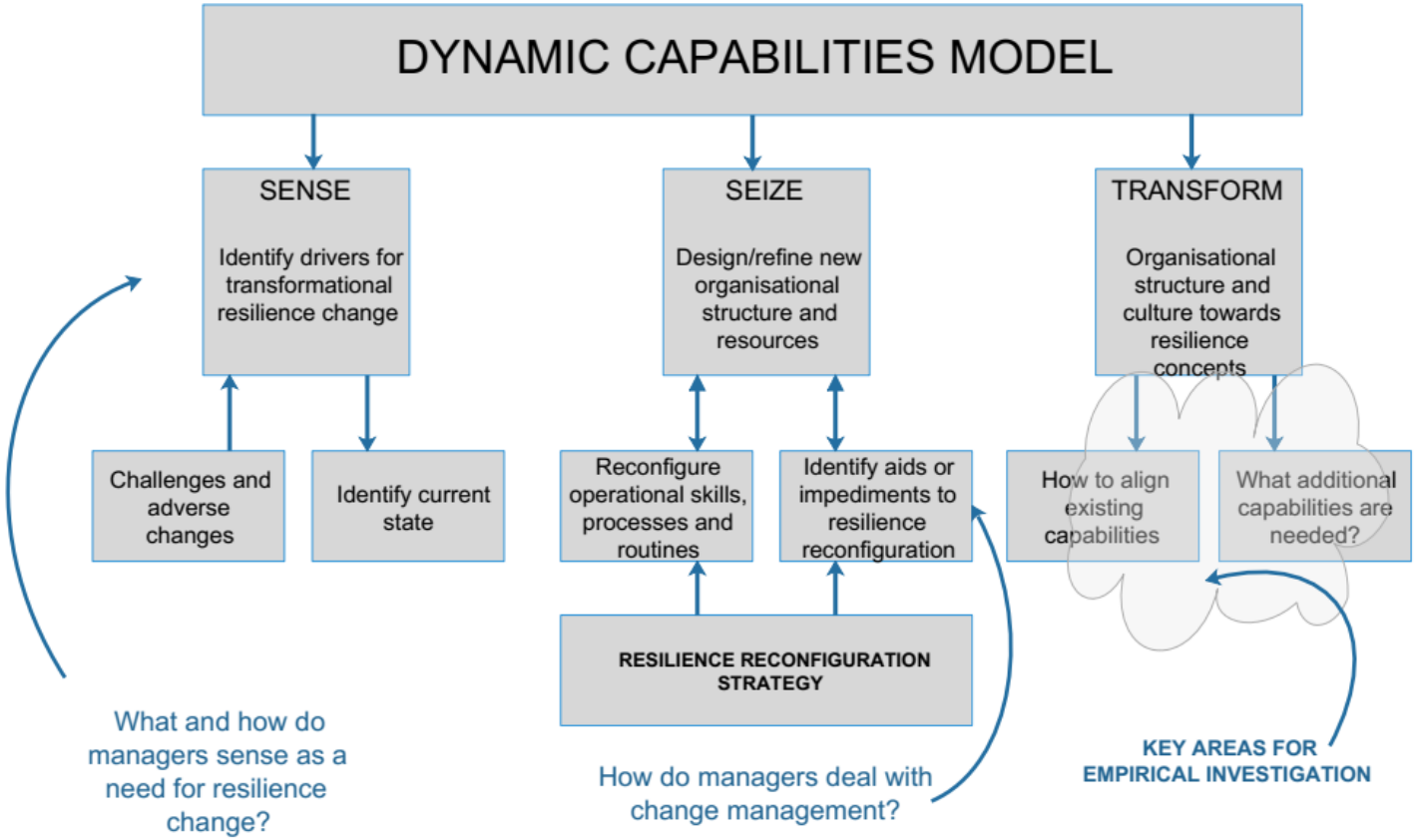


Figure 9-3: Dynamic capabilities model for transforming and reconfiguring organisational resilience (Adapted from Teece 2017).

9.5. Findings from the empirical research

This empirical research focuses on establishing a clearer understanding of how the dynamics of disruptive change are managed within the contemporary Australian port's risk management capabilities and processes (Davidson *et al.* 2016; Haraguchi, Lall & Watanabe 2016). The investigation explores the extent and capabilities of risk management knowledge, capabilities and capacities of senior executives charged with managing port authorities and government instrumentalities overseeing Australia's 70 larger ports (Ports Australia 2017).

In general answer to the primary research question, the empirical research showed that port risk management processes appear to be based on sound management principles. Australian ports cope best against physically manifested disruptions (storms, oil and chemical spills, infrastructure damage), but their effectiveness levels reduce markedly against the more intangible disruptions arising from deliberate human interventions such as security breaches, cyber-threat, criminality, and socio-political acts. In general, Australian ports demonstrate mixed levels of competencies in managing the risks and consequences arising from low probability/high consequence disruptions as will now be discussed.

9.5.1. Risk management competencies

The primary research question asks how the ports manage risks and consequences arising from low probability/high consequence disruptions, and this question encompasses port risk management processes, procedures and resources, and the primary resource consists of the management complement and their competencies. The findings indicate that Australian ports effectively manage physically manifested disruptions (storms, oil and chemical spills, infrastructure damage) but effectiveness levels reduce when challenged by deliberate human interventions (security breaches, cyber-threat, criminality, socio-political acts). This effectiveness variance is shown by the surveyed port managers reporting between 56-80% effectiveness in managing individual categories of disruption, with lowest levels of effectiveness recorded against security breaches and the failure of crucial goods and service supply (Section

7.6). The highest numbers of effective responses were recorded against hazards derived from human causality, adverse natural events, operational plant and equipment failure, and ship incidents. Respondents who reported difficulties in coping found their most challenging hazards to be infrastructure failure, adverse natural events, and adverse socio-political events. The lowest level of disruption management effectiveness (31%) was experienced against security breaches.

The research did not find significant associations between levels of risk management competency and the levels of risk management qualifications. Not all senior port executives hold risk management qualifications, despite their important risk management decision-making roles. The literature provides scant information on port managers without formal risk management qualifications, including port procedures for risk management professional development, the quality of in-house training programs, and the levels of reliability and adequacy of risk management strategies, plans and policies produced by managers without risk management qualifications. Workplace experience and training is necessary for the full development of port management leadership capabilities, but further competence would likely arise from 'continuously implemented and empowered' formal training to provide currency in underlying technical skills (Manuti *et al.* 2015, p. 1).

9.5.2. Port vulnerabilities

The research found that port managers' highest-ranked reason for developing resilience capabilities was to gain a better understanding of the risk environment and resultant port vulnerabilities, and to thereby enable improved detection of potentially disruptive events (Subsections 8.3.2.; 8.3.4.). Port managers indicate in their survey responses that they were mindful and aware of their risk environment and of the types and regularity of disruptions experienced during the past five years. They expect fewer port disruptions to occur across most known categories of risk during the next five years, and only three risk types to increase: cyber-threats, socio-political issues and financial risks. Conversely, deep uncertainties are reported by these managers

concerning their port vulnerabilities to new and emerging risks, whose causalities and potential disruption consequences are yet unknown.

Where experience of disruptions might be expected to shape managers' expectations of future port vulnerabilities, this was not apparent from the survey. Figure 9-4 (reconfigured from previous Figure 7-5) compares the types and numbers of disruptions previously experienced by respondents with what these port managers predict for the short-term future. Previously, three types of occurrence predominated - operational or equipment failure, adverse natural event, and infrastructure/superstructure failure. However, approximately half of respondents discounted the likelihood of these adverse events reoccurring in the near term. Alternatively, socio-political and financial risks are elevated beyond past low-level occurrences. This leads to a possibility that if management assumptions about types and likelihood of future risks are incorrect, then their scope of controls and responses might be inappropriate.

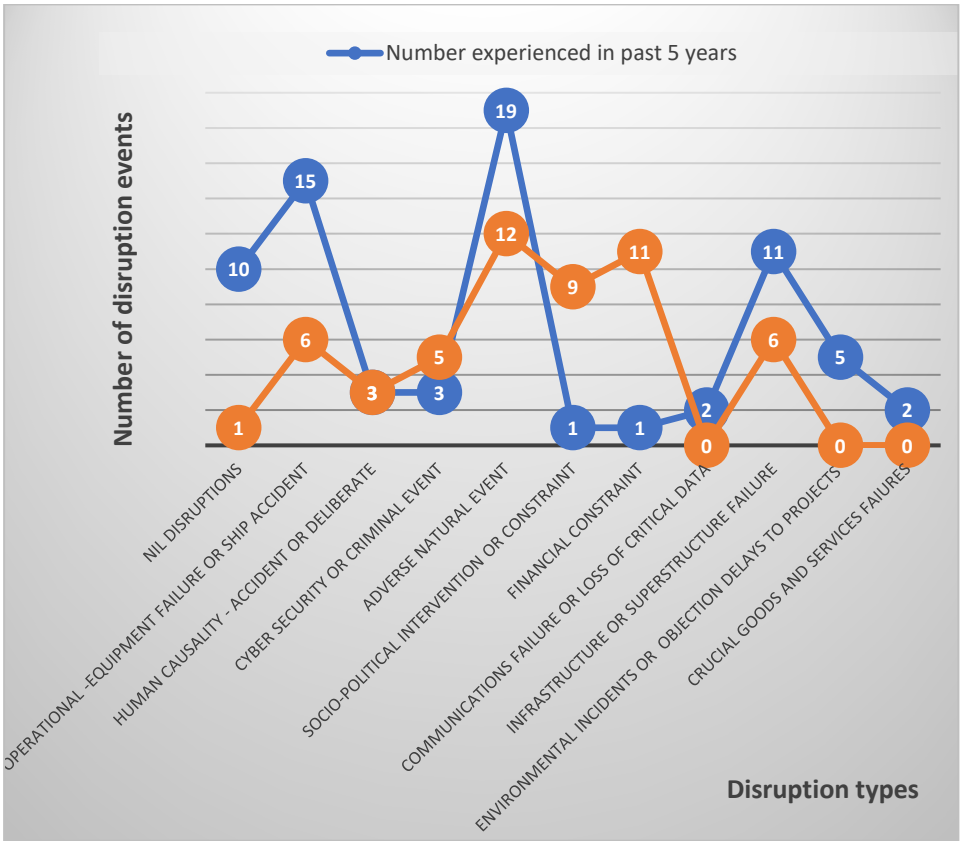


Figure 9-4: Comparison between historic and predicted port disruptions (Author).

The research also assessed how much reliance port managers might place on insurance as a means of spreading risk. Respondents reported from their

experiences that port operators should concentrate on strengthening their risk management capabilities, rather than look to insurance as either a risk transfer opportunity or a source of financial assistance towards disruption recovery. O'Hare, White and Connelly (2016) suggest that reliance upon insurance is a counterproductive resilience measure in that it creates a mindset that more readily accepts risky behaviour and resists change after crises. White and Connelly argue that a reliance upon insurance is more attuned to an organisational return to the status-quo rather than organisational adaptive reconfiguration. Nonetheless, with ports' increasing exposure to multiple hazards, insurance remains an important resilience technique in financing a port recovery within some categories of risk (Lam & Lassa 2017),

9.5.3. Operationalising resilience

The findings from Section 8.4 demonstrate respondents acknowledgement that resilience:

a) is their responsibility;
b) is not too complex to implement and offers business continuity benefits;
c) offers tangible gains and competitive advantages;
d) is not too expensive to implement; and
e) implementation is not impeded by change management, confidentiality or industrial relations barriers.

However, the reality is that 50% of the respondents believe that they can adequately cope with future disruptions by employing current risk management practices, whereas the situation actualities suggest that they cannot. The remaining 50% recognise that risk management change is required.

Respondents reported that the most important driver for resilience change at their ports would be the Board and senior management championing the concept. Few respondents believe that climate change is a feasible driver for resilience change, which is inconsistent with the many climate change studies

that explore resilience as a means of risk mitigation (for example, Becker *et al.* 2015; Chhetri *et al*. 2015; McEvoy & Mullett 2015). Port managers generally acknowledge the possibility of increasingly severe natural events, so that their rationale for ranking climate change as an unimportant driver for resilience enhancement remains unclear. Drivers for resilience change only initiate the operationalising process and so the research investigated how progress could be made in achieving transformational resilience change. Requisite steps towards operationalising resilience through transformation and reconfiguration are now explained with the assistance of the proposed dynamic capabilities model from the literature survey findings highlighted in Subsection 9.4.4.1

9.6. Transforming and reconfiguring port resilience capabilities

The purposes of the current study included an assessment of what ports need to change in their practices to become more resilient (secondary research question two), and this assessment provides insights towards a pragmatic and practical understanding of what port managers must undertake to achieve transformational resilience change, and how they might proceed through the sense, seize and transform process as a workable management systems strategy (Teece, Pisano & Shuen 1997; Teece 2018). This explanation is undertaken firstly by examining the individual components of the dynamic capabilities model developed from the literature review (Subsection 9.4.4.1) and then fitting the empirical findings to the model.

9.6.1. Sensing drivers for transformational resilience change

The data provides evidence that what port managers recognise as catalysts for resilience change precipitates an organisational shift towards a strengthened resilience state. This aspect of the dynamic capabilities model is shown in Figure 9-5. In the event of port management 'sensing' the need for resilience change, then this motivation is related to possible opportunities to be derived from the process, because if there was to be no gain and with no regulatory compliance to enforce the process, then there is little rationale for change. As described by Winter (2003, p. 994):

If opportunities for competitively significant change are sparse enough or expensive enough to realize, then the added cost of dynamic capabilities will not be matched by corresponding benefits.

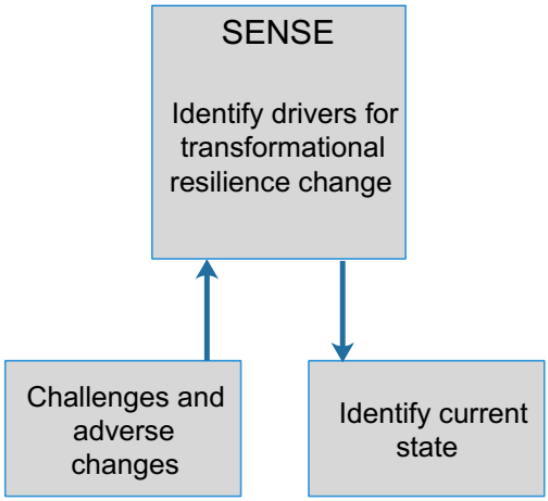


Figure 9-5: The process of sensing opportunities for transformational port resilience change (Adapted from Teece 2017).

Drivers for port resilience change are regarded as catalysts for the process, and the derived opportunities form part of the outcomes. Enhanced port resilience leads towards safer ports, within the charter party 'safe port' definition (Girvin 2017). Safer ports arise through management achieving a lower frequency of disruptions, faster recovery times from disruptions, and a reduced likelihood of delays for visiting ships. This also equates to increased productivity through reduced port downtime, increased cargo throughput, and a more effective use of resources. Increased port productivity is a sign of port efficiencies, and Girvin (2017) notes the commercial benefits of a safer port by quoting (p. 2) 'a well-worn truism: time is money'. In 2016-17 Australia exported 818 million tonnes of iron ore at an average US$68 per tonne (Culley 2018). A productivity increase of one day per year by each iron ore export port could potentially increase the export volume by two million tonnes. Port resilience and derived efficiencies also potentially offers competitive advantage against ports of other nations, which also vie for opportunities to ship natural resources (for example iron ore and coal) to Asia (Reynolds 2010). In short, port managers might feasibly 'sense' competitive advantages in seizing opportunities to become more resilient (Reynolds 2010; Piening 2013; Teece 2017).

This thesis finds that ample scope exists for Australian port managers to derive opportunities from transformational resilience change. Respondents to the empirical research acknowledge that their risk environment severely challenges existing risk competencies, and as discussed in S 7.6, port managers' effectiveness in managing all disruption categories is self-reported to vary widely. Up to 29% of ports required external assistance in managing these categories of disruptions, and depending on the disruption type, up to 28% of respondents are unsure of their capabilities and capacities to respond and manage. The port risk environment is predicted to become more challenging with new and increasingly severe hazards (WEF 2018). However, there appears to be limited likelihood of port transformational change arising specifically from perceptions of a changing risk environment. Respondents generally predict fewer disruptions to arise in the future, and considerably so for crucial goods and services supplier failures (Figure 9-4). A major challenge for port industry resilience change, as identified from the research, is that 50% of respondents reject the need to amend or divert from their current risk management practices, despite some reportedly low levels of risk management effectiveness.

Respondent sensing capabilities are likely in need of focused education towards improved risk identification and analysis capabilities. The research demographics (Section 7.4) identify that 13.5% of port senior executives within the survey do not hold any risk management qualifications, and 48% of respondents have gained their risk management expertise from workplace experience and/or in-house training. Overcoming this high level of resistance to resilience change might begin with an increased industry focus on risk management education and training. The sensing process also incorporates identification of drivers for resilience change. As discussed, the respondents identified ample reasons for change in the form of tangible gains, enhanced business continuity, competitive advances and low costs to achieve the ensuing benefits. If transformation and reconfiguration is to occur, then respondents sense that influential drivers to initiate this process will likely include customer

pressures and the threat of financial loss or market share, government encouragement of change, and societal demands for safer operations.

A final step in the sensing process is an accurate identification of the current state of port risk management capabilities, vulnerabilities and awareness of the risk environment. If some managers are either unable or unwilling to accurately articulate what their current resilience state might be, then their abilities to identify what needs to be changed is undoubtedly questionable. The empirical data clearly shows that 50% of the respondents do not accept the need for change, and yet even the best performing ports are achieving a maximum 80% level of effectiveness against disruptions. The respondents fail to demonstrate uniformity and in their risk identification and vulnerability processes, with the possibility of some respondents demonstrating a risk myopia outlook towards future risks, an outlook that appears to sit comfortably with a reluctance for change. The port industry has access to a peak industry body which has previously developed safety and risk management guidelines for the ports, and regularly convenes representative working groups to address risk in all major areas of port activities (Ports Australia 2018). A useful and in-house approach to identifying the current port resilience state might commence with a peak body working group study. Once the sensing process that identifies the need for transformational change is completed, then the processes involved for reconfiguration need to be identified.

9.6.2. Seizing the means for reconfiguring resilience strategies

To gain the benefits of a dynamic capabilities seizing process (Teece 2018) port managers must identify the necessary skills, processes and routines to enable resilience change; to strategise what organisational structural changes become necessary and what resources might assist the processes, and to explore what impediments must be overcome, as shown in Figure 9-6. This is an ongoing process, because the port and its operations are continually evolving and adapting, and these changes create new sources of vulnerability. All respondents to the research agree that the impetus to configure skills, processes and routines to enable resilience change is driven by top-down

advocacy and oversight, however before this process can be effectively implemented the Board and senior executives must become sufficiently cognisant of what is required and how best to initiate the enabling processes.

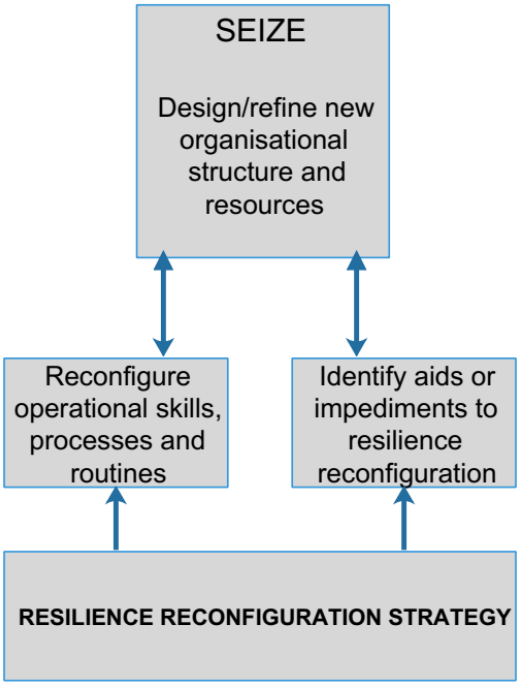


Figure 9-6: Seizing capabilities for resilience transformation and reconfiguration (Adapted from Teece 2017).

Restructuring the port organisation likely involves evaluating the extent of bureaucratic command and control constraints within the port's strategies, plans and policies as discussed in Section 5.7. Some bureaucratic management restructuring and reconfiguration may be found necessary to delegate sufficient authority, autonomy and flexibility to responders who operate within the emergency management framework (Section 5.7). Further, resilience must be set as a corporate objective to empower and maintain the reconfiguration process, and for a future resilient state to be achieved, then enabling strategies must be assigned towards this corporate aim. The port management policies and culture may need to be modified to ensure that strategic, tactical and operational level capabilities exist for resilient day-to-day operations, plus a resilient response and recovery capability in reserve to deal with crises situations as outlined in Section 7.8. The literature advises that resilient organisation structure is based upon the creation of flexible, adaptive and joined-up teams, with emphasis given to developing the leadership strengths

and capabilities of frontline response teams who must operate closely in emergencies largely independently of senior management (Worboys 2015; Hayes & Owen 2017). However, seven respondents reported that their present organisation structure is dependent upon external services providers and internal contactors for the provision of key services such as IT. These respondents find difficulties in communicating with and controlling these external and internal services providers, who demonstrate differing levels of risk management training and perspectives on risk management to the port employees (Sections 7.8.6.; 7.8.9.). If these independent services providers constitute a source of vulnerability to the port's business continuity effectiveness, then ports should consider the feasibility of engaging personnel in-house to provide these key resources and capabilities.

IT management is potentially a case in point for port organisational restructuring if the port does not already employ an IT professional. A port IT professional requires knowledge and skills associated with the implementation of ISO/IEC 27031:2011 (IT business continuity), and ISO/IEC 27032:2012 (cyber-security) in operational environments. With cyber-threats an increasingly threatening issue for ports, as experienced by the Maersk organisation in its global port operations (Roth & Nakashima 2017; Meyer-Larsen & Müller 2018) then engaging a competent in-house IT professional may change from being a costly extravagance to a necessity if future resilience is sought. The study shows that 65% of respondents (*n* = 38, 65% = 25) experienced security breaches during the past five years, sufficient to affect the reliability of their port operations, resources, capabilities and infrastructure. Forty percent (10) of these 25 respondents reported difficulties in coping with these security breaches. Accordingly, and with Australian businesses coming under increased regulatory, public and socio-political oversight (Hooper *et al.* 2018), ports might consider the engagement of a dedicated risk management officer. A further benefit with in-house specialists working alongside and assisting other managers is that a measure of these specialists' knowledge and skills might gradually spread across the wider management structure.

9.6.2.1. Reconfiguring competencies and organisational structure

The future practice of port risk management is challenged by a continually evolving risk environment that creates increasingly sophisticated and numerous risks (WEF 2018) as with cyber-threats (Hopkin 2017; Meyer-Larsen & Müller 2018). Preparedness to treat new, emerging and unforeseen risks, which might impact quickly and unexpectedly, requires increasingly far sighted and sophisticated micro-foundations for developing effective risk management capabilities and capacities. Port managers who just a decade ago might have employed risk management primarily against financial and legal liability are now addressing strategic and operational risks within much wider skill sets. Accordingly, this thesis concludes that port managers must become increasingly familiar with multiple risk management artefacts, inclusive of safety planning and process, emergency response, risk mitigation, disruption management, business continuity, and corporate adaptability.

Port risk management and resilience is not just the province of a specific risk manager or Chief Risk Officer, rather, ports have a holistic need for risk-based process by all managers in all departments within every aspect of management (Haimes 2016). Effective risk-oriented port decision-making processes are likely to become dependent upon all managers acquiring risk management awareness, professional risk management knowledge, and a culture of continuous risk management improvement. Learning and continuous improvement are important, because the risk environment is not a static problem. The dynamic nature of port risk ultimately requires periodic reconfiguration of risk management competencies, which involves an understanding of which elements must be changed for successful transformation to occur. The micro-foundations of this process at Table 9-2 conceptually describe these elements, and outline the management skill-sets, capabilities and routines that might enable future safe-port management.

Disruption categories	Risk management skills	Risk management processes	Risk management procedures	Risk management structure	Decision-making rules	Collaboration and communications	Risk management resources
Adverse natural events; Climate change; Criminality; Cyber security; Environmental pollution; Failure of crucial goods and services supply; Financial crisis; Human causality – accidental or deliberate; ICT failures; Inability to manage new technologies; Infrastructure failure; Loss or theft of critical data; Operational equipment failure or ship accident; Pandemic/disease; Socio-political intervention or constraint; Terrorism; Unknown risks.	Risk management academic qualifications; Port industry knowledge; Capacities for learning; Enterprise risk management; Timely access to risk information; Risk governance; Abilities in critical analysis and strategic thinking; Communication and collaboration skills with internal and external stakeholders; Conversant with risk management and analytic software; Conversant with digital and data technology use and safeguards.	Management of strategic, tactical and operational measures and enhancements; Maintaining constant awareness and monitoring of the operational and risk environments; Ensuring that all management systems, procedures, and routines are fit for task; Ensuring compliance with regulatory and industry requirements; Ongoing R&D, and monitor external science and technology developments; Monitor supplier and customer innovations, needs and requirements.	Decision-making protocols; Establish parameters and controls; Advocacy and commitment; Documented procedures as risk controls; Quality management to optimise socio-political and regulatory compliance requirements, including climate change emissions; Internal and external audit procedures; Competency indicators and institute procedures for monitoring and evaluating progress; Learning and iteration procedures.	Structure based on aligned corporate governance and risk governance policies to ensure adequacy of managerial interactions and compliance; Structure enables integrated treatment of risk, not fragmented – an 'all-risk' model; Structure follows a sound risk management policy and framework; Continuous alignment and realignment of tangible and intangible assets and resources;	Risk management compliance and alignment with rules, regulations, standards, codes of practice, laws, societal standards and ethical considerations; Boundaries are established within the governance policy and business model which establish internal limits on management decision-making. Decision-making rules need to be monitored to avoid unnecessary constraints and organisational rigidities.	Inter-organisation collaboration and communication to break down silos; Collaboration across the organisation to develop a holistic perspective of risk and vulnerabilities	Intangible risk management resources include staff knowledge, skills and experience, competencies, systems and technology; Tangible risk management resources include physical attributes, infrastructure, superstructure, plant, equipment and stores; Strategies, plans and policies.

Table 9-2: Conceptual management competencies and organisational capabilities for future safe-port management (Adapted from Teece 2007; Hopkin 2017).

Additionally, structural changes may be required across the port's physical resources to better meet the challenges of an increasingly adverse risk environment. Stronger storm events, storm surges and possibilities of tsunami waves might necessitate redesign and strengthening of wharves and ship mooring devices to withstand increased loads on fenders and mooring line bollards and hooks (Tsinker 2004, 2014). Operator control areas in buildings and machinery such as cranes may need to be airconditioned if increasingly warmer temperatures create workplace stress.

Ports also need to look towards potential impediments for resilience change, and from the empirical research, the chief impediment appears to be unwillingness for change, with 50% of respondents preferring to persist with existing risk management processes and techniques rather than reconfiguration towards strengthened resilience (Subsection 8.4.3). For resilience change to become essential for such a high proportion of respondents, a possibility exists that either legislative compliance measures are needed, or the occurrence of a disruption that becomes a focusing event for change. A focusing event is described by Birkland and Warnement (2017) as a crisis, disaster or catastrophe that is disruptive, sudden, unexpected, geographically centred, and widely noticed and reported across public and private domains. Focusing events with relevance to global port risk and security management changes arguably include the 9/11 terrorist attack, the 2008 financial crisis, hurricanes Katrina and Sandy, and large oil spills resulting from the *Exxon Valdez* and *Sea Empress* groundings. Given that Australian ports are ready to transform and reconfigure their existing risk management culture, structures and practices towards enhanced resilience concepts, then the transformation process needs to be understood.

9.6.3. Transformation towards enhanced port resilience

Transformational change may be difficult for the port bureaucratic mindset (Everett 2003a; Pettitt 2014) because port managers may prefer a known, stable and predictable operating environment rather than a reconfigured, more flexible and adaptive organisational structure with a culture of

continuous resilience renewal (Piening 2013; Teece 2017). Australian port authorities as corporatised state government entities can engage in transformational change, with Boards of Directors empowered to determine the policies and control the affairs of the port authority (see for example Division 2, S 8 of the *Western Australia Port Authorities Act 1999* (DoT-WA 1999). The Board will likely keep the Minister informed of any major changes that are planned and might choose to outline the intended activities within the port authority's annual statement of corporate intent. Conceptual managerial transformation towards a port resilience culture is shown in Figure 9-8. A key aspect of implementing dynamic capabilities theory towards future resilience is that existing tangible and intangible capabilities, assets and resources should be maintained, and where necessary enhanced (Teece, Pisano & Shuen 1997; Teece 2017).

Figure 9-8: Organisational transformation (Adapted from Teece 2007).

This thesis survey found that Australian port risk management concepts are generally based on the ISO 31000:2018 risk management standard. However, port risk managers' execution of these capabilities seemingly requires attention, as borne out by the wide variance (56-80%) in effective port risk management outcomes across a range of risk environment hazards (Section 7.6). Within a dynamic capabilities context, transformation of the port structure and culture towards resilience concepts is assumed to be constructed upon the existing risk management foundation, and in the case of some Australian ports these foundations need reinforcing. Accordingly, a necessary

precursor activity within the transformation process should be to optimise port risk management competencies. An early improvement might be enabled through increased managerial understandings of the various risk, resilience and business continuity standards.

In assessing what additional port capabilities are required to achieve future resilience, port managers know what risk management capabilities, capacities and resources exist and have it within their power to modify these capabilities. The survey respondents reported diverse proficiencies in risk management knowledge, capabilities and competencies, and so there is little likelihood of a 'one-size-fits-all resolution of the resilience transformation process. Instead, Chapters 4 and 5 provide academic and practitioner guidance to the state of the knowledge, and frameworks and maturity models by which to gauge where each port sits within risk and resilience management evolution. From these guides, port managers are assisted in assessing what is needed to take their next steps towards resilience capability transformation and reconfiguration.

In summation, evidence exists that much remains to be addressed within an investigation of port disruption management and the operationalisation of resilience concepts into mainstream port practices. The tentative contributions that this research makes to the knowledge are outlined in the next section.

9.7. Contributions to knowledge

This study has found that Australian ports have difficulties in managing a changing risk environment that is characterised by new and unexpected categories of hazards, and increasingly severe natural hazards. The second major finding is that while port managers have the foundational capabilities to operationalise resilience, they are unclear about the processes and procedures required for progression to a higher resilience state. The study investigates Australian port risk and resilience competencies from two directions, namely how port managers presently manage low probability, high consequence disruptions, and how they might manage future risks that are characterised by uncertainties, unexpectedness and unknowns. The latter investigation focuses

upon the operationalisation of resilience, and in relation to port managers' difficulties in understanding resilience transformation processes, a contribution to the knowledge is made by adapting Dynamic Capabilities theory towards this investigation.

The thesis approaches port resilience differently, by examining the processes that enable future port resilience, and how existing port management capabilities and competencies alone are insufficient to achieve this goal. The thesis proposes that capabilities are not so much the issue in the port transition towards a higher level of resilience. Instead, port managers' capabilities for reconfiguring towards a future resilience state are dependent on their ability to engage in the processes for sensing and seizing the opportunities for transformation. Accordingly, the contribution of this research is to recognise the building of port resilience as a process that is supported by port management capabilities.

This thesis also shows that dynamic capabilities theory (Teece, Pisano & Shuen 1997; Teece 2007, 2017, 2018) and systems theory have inter-relationships with resilience concepts (for example, flexibility, complexity, innovation, adaptiveness, improvisation, transformation, learning, coping with threats and sudden change, managing uncertainty, systemic change, situational awareness, dynamic processes, governance and leadership). Lesser theoretical contributions include the development of proposed descriptive models for a port risk management framework, a port resilience framework, a port risk management capabilities maturity model, and a port resilience implementation model. These models were adapted from other fields of research and reconfigured within a specific port-centric context to help understand and answer the relevant aspects of research questions.

9.7.1. Implications of safe ports and resilience

This thesis takes an adaptive conceptual approach towards understanding how resilience might be operationalised from a pragmatic port management perspective. An analysis of Australian port managers' perspectives on organisational resilience and transformation for strategic advantage follows an

investigative pathway that is suggested by Teece (2007). This pathway was used in developing a port-oriented resilience management framework to assist academics and port managers in better understanding the evolution, implementation and maintenance of resilience management practices. The value of such an approach is outlined by Teece (2007, p. 1319) as a means of establishing clarity in how an organisation:

a) 'senses and shapes opportunities and threats;
b) seizes opportunities; and
c) maintains competitiveness through enhancing, combining, protecting, and when necessary, reconfiguring the business enterprise's intangible and tangible assets.'

The title of this thesis is 'Safe Ports for the 21st Century: Australian port resilience'. From a port management perspective, the notion or need of a 'safe port' is driven by the charter party legal agreement between the charterer and the shipowner (Girvin 2017). Port managers have long been peripheral to 'safe port' discussions (and ensuing legal arguments) as described by Astle (1996) and Mandaraka-Sheppard (2014). However, there is no guarantee that port managers will continue to be a largely silent participant in safe port arbitration, and if legal intervention occurs then a possibility exists that multiple aspects of providing a safe port will become port management compliance risks. Where supply chains have experienced ship traffic congestion following Australian port disruptions, the cost to global trade has been high, with lost sales reportedly costing up to US$100 million per day for larger ports (Loh & Thai 2015). According to the World Economic Forum (WEF 2018), future hazards inclusive of cyber-threats, adverse natural events, financial and climate change disruptions are likely to increase in frequency, which will likely exacerbate ship delays at ports. If an increased frequency of disruptions instigates supply chain pressure on the Australian government and port private sector interests to do more to make port operations more resilient, then the port risk management task will change. Consequential or proactive measures to make port operations more effective within a ship visit context would require a reconfiguration of

intangible assets, routines and resources to enable compliance. Port management critical thinking and risk analysis is a necessary component of 'sensing 'potential changes in the wind, as outlined in the following section.

9.7.2. Management implications

This thesis contributes to academic and practitioner understandings of the internal and external risk environment and future threats to future port business continuity. The external risk environment is explained to include the potential for systemic risks to affect crucial goods, services and infrastructure within a port's onshore and offshore regional areas. The thesis stresses the importance of resilience not only in port management responses to crises but also in day-to-day emergency situations for achieving maritime logistics and transportation competitive advantage. The research underlines how resilience has multiple dimensions and capabilities (for example, flexibility, complexity, innovation, adaptiveness, and improvisation) that become either individual or combined risk management tools in a port's disruption management repository. A Dynamic Capabilities approach to risk and resilience management provides practitioners with a readily understood blueprint for understanding and formulating what needs to be done for managing and responding to new and emerging risks and uncertainties. The macro-findings from the employment of a dynamic capabilities approach suggest that a similar approach may be useful in other areas of critical infrastructure and transportation resilience research.

Importantly, the findings suggest that port managers are insufficiently proactive in managing risk and achieving increased resilience. Remedial steps would involve auditing the port against risk management and resilience provisions of ISO 31000:2018 and ISO 22316:2017, and upon receipt of the findings, assess the capability gaps and rectify the perceived shortfalls. This may include adding new skill sets to the management team, for example engaging an IT professional to manage the risk of cyber-threats. A review of predicted risks and the potential transmuting of port risks from climate change (for example higher temperatures, new diseases, stronger winds, worse floods,

higher storm surges) leads to the need for new emergency response plans, changed work practices, and revision of occupational safety, health and environmental protection plans, policies and practices. Several high-level managers lack risk management training and qualifications, and Boards of Directors should address this shortfall because it leaves the directors without evidence-based information that they require to make correct risk and resilience management governance and policy decisions. Directors are responsible for establishing the port's tolerance and attitude to risk, and with some ports reporting a disruption management efficiency of less than 60% then the relevant ports' risk and audit committees should re-evaluate management competencies and performance in the areas of contingency management and business continuity. These are all indications that sufficient risk management activity is carried out in Australian ports to ensure that port managers meet their levels of regulatory compliance and have mandatory systems in place, but there is no surveillance to ensure that port risk management outcomes meet the lowest levels of international standards.

An implication of this research for port managers is that they should assign greater emphasis towards managing and coping with conceptual risks and their consequences. Australian port managers are more aware and proactive in monitoring and managing the risks of those hazards with physical and measurable attributes, for example storms associated with adverse natural events. Conceptual risks are those that manifest from non-tangible hazards, whose risks often emerge unexpectedly – for example port hazards involving security breaches, cyber-threats, criminality and socio-political acts.

Port managers agree on the value of resilience to their organisations but half of those surveyed intend remaining with their existing risk management processes and procedures, which potentially leaves them under prepared to manage unknown risks and deep uncertainty. New and emerging hazards that are associated with unknown risks and deep uncertainty require innovative, adaptive and flexible responses inherent with resilience, and these response characteristics cannot be provided by traditional risk management. Port

managers can gain further competencies in managing new and unexpected risks through familiarization with, and subsequent implementation of Dynamic Capabilities Theory. Dynamic capabilities can assist organisations towards transforming and reconfiguring their risk management capabilities towards organisational resilience (Teece 2017a, 2018). Enhancing port management competencies and organisational capabilities is part of this transformation and reconfiguration process.

Other findings of this thesis are listed in the preceding chapters.

9.8. Study limitations

The sample size is a limitation that would caution against generalisability to the wider international port management community. Further, the research is integrated in systems thinking, resilience and dynamic capabilities theory (Vogus & Sutcliffe 2007; Teece 2017) and differing outcomes might arise, or important factors within this thesis become overlooked, if the study were to be grounded in another research approach. However, due care was taken to minimise the influence of extraneous variables to ensure that research results were internally valid and replicable. It was assumed that responses to the research survey questionnaire were honest and accurate, however recognition is made that respondent self-reports reflect the potentially subjective nature of their risk management and resilience environment interpretations.

The scope of the study embraces Australian port managers associated with 27 port authorities and State government port management departments geographically spread around the Australian coastline. This narrowing of the study population is intended to make the research aims more feasible and manageable, however this geographical focus on Australia limits the number of managers available to the survey processes and inhibits the generalisability of findings to global ports. A possibility exists that non-respondents to the survey possess knowledge or exhibit risk management behaviour that differs from respondents and is not reflected in the data, and thereby constitutes a limitation of the study.

The sample size affected the researcher's ability to conduct some quantitative data analysis tests, the statistical significance of some findings, and the internal consistency of some survey questions. Question responses or components of responses with a low Cronbach Alpha reliability coefficient were either revised or discarded (Tavakol & Dennick 2011).

An early higher degree by research challenge involving this supervised research project arose from initially relying on the scholar-practitioner's 30-years of experience and deep knowledge of port management practices, as opposed to investigating practical aspects of port operations within the academic literature. This demonstrated at an early stage the importance of an evidence-based rather than values-based approach to research (Short & Shindell 2009). Initially the control method resulted in over-correction, with too many references being employed. A further challenge was revealed when time came to choose research methodology, because the researcher's extensive relationships with Australia's senior port managers suggested that potential existed for either surveyor bias or respondent bias if telephone or face-to-face surveys were employed. Instead the researcher chose a web-based survey research technique.

9.9. Implications for future research and practice

The research findings tentatively outline a different perspective of port resilience thinking, behaviour and conceptualisations than what are provided by current theories and Australian government resilience viewpoints (TISN 2016). Instead, port managers demonstrate a more pragmatic and non-theoretical viewpoint of resilience implementation and its value to them, and some express their resistance to the prospect of resilience changes. To some extent these research findings mirror those from a study of US port risk management practices (Rice & Trepte 2012). Confirmation of these tentative findings suggests the need for a deeper and more vigorous gathering of data, extending to case studies and workshops, and further study to either modify, expand or reject the present findings.

New findings from this thesis appear to take the port risk management domain in new directions to existing theory and practice, and potentially creating possibilities for further investigation. Future research might advantageously identify areas of professional education where theory might be translated into useful practical knowledge, and disruption preparedness. There is much within this research field that is both challenging and relevant to Australian government initiatives in promoting resilience as critical infrastructure protection. The topic is also potentially relevant an academic companion to the work of the newly instituted Australian Department of Home Security. Much remains to be researched within this field, but the researcher was cognisant of keeping the task to a manageable size within time and resources constraints. However, opportunity was taken during the thesis journey to produce journal articles, conference papers and a book chapter related to interesting and associated findings along the way, closely related to the thesis topic.

Resilience capability maturity modelling might be furthered by investigators in the following forms:

a) identifying further or alternative inputs to the model from best practices/standards/expert knowledge;
b) considering whether a port resilience maturity model might be best managed with a software system;
c) Employing Bayes theorem to extend the research in this field, particularly in relation to known unknowns and path dependency; and,
d) whether from a governance and ethics perspective, maturity model designs and achievement measurements should be performed in-house or by a third-party assessor (Carralli, Knight & Montgomery 2012).

9.9.1. Future research agenda

Opportunities for future research arise from this study. Future studies that increase port resilience knowledge are likely to benefit both academics and practitioners. Translations of improved risk management and resilience theory into practical concepts have potential to benefit port reliability, supply chain competitiveness and regional economies. Port managers' lack of encounters

with some disruption categories during the past five years is of specific interest as a basis for further study, within the contexts of:

a) Does a lack of experience with managing unfamiliar risks leaves the port more vulnerable should such an event arise;
b) If an Australian port is in a geographical area where some hydro-meteorological hazards might not normally exist, then might the effects of climate change make such hazards more likely, and how might the port prepare – for example, to address new risks of tropical cyclones and tropical diseases that might ultimately impact more southerly ports; or,
c) Whether a source of disruption (for example cyber-attack) that is yet to occur might lead to port risk complacency regarding relevant disruption preparedness.

Further research might investigate whether an association exists between senior port managers without formal risk management qualifications, and the effectiveness of port disruption management outcomes. The research could also determine the implications of managers without formal risk management qualifications having responsibilities for authorising and arranging the organisational risk management professional development and in-house training programs for others. The suggested exploration might also assess the reliability and adequacy of risk management strategies, plans and policies produced by managers without risk management qualifications.

Post-doctoral studies to advance the knowledge might benefit from deeper immersion into individual port authority disruption records, for example emergency operations logs where decision-maker activities, actions and some indications of informed decision-making are detailed (Lansdale 2012; DoT-WA 2015). Each State has legislative requirements for their ports to raise and retain records to cover multiple aspects of significant port incidents (QSA 2013; DoT-WA 2015) and access to such documents would undoubtedly provide more detailed evidence of port resilience behaviour.

Whereas the present research employed a mixed methods technique in exploring, confirming and generating risk management and resilience theory, future research might consider an expanded research project by employing either quantitative or qualitative approaches.

Future research might also investigate why half of the management respondents consider that existing risk management practices suffice for their needs, despite evidence that existing risk management plans and strategies fail to produce effective outcomes against certain disruption categories. A focussed exploratory emphasis could be directed towards examining why such an attitude exists, why it is so widely demonstrated, what realities prompt these managerial assumptions, what real costs and effort are required to strengthen resilience levels in Australian ports, and what potential benefits might accrue from such a research program to the ports, their region, and to the national economy.

Australian port managers are shown to be optimistic in predicting fewer disruptions for the short-term future than they have experienced during the past five years, and consequent research might seek to validate or disprove these practitioner expectations.

Future research that benefits the understanding and practice of port management is a worthwhile process, to the Australian economy and to global trade, with ports enabling the export of AU$208 billion in energy and resource commodities in 2016-17. Academic studies in areas like risk management and resilience pave the way for increased practitioner understandings, and potentially contribute to port efficiencies, effectiveness and competences. If that is the case with this thesis, then the long, hard journey is worthwhile.

References

Abbas, R., *et al.* (2018). "Pinpointing what is wrong with cross-agency collaboration in disaster healthcare." Journal of the International Society for Telemedicine and eHealth **6**(1): 3-1-10).

Abdussamie, N., *et al.* (2018). "Operational risk assessment of offshore transport barges." Ocean Engineering **156**: 333-346.

ABS (2017). Key government finance statistics: Accrual operating results, ABS Statistics. Canberra, ACT, Australian Government.

Accenture (2015). Accenture 2015 Global Risk Management Study. North American Insurance Report - Paths to Prosperity. Washington, US, Accenture Finance & Risk Services.

Acciaro, M. (2015). "Corporate responsibility and value creation in the port sector." International Journal of Logistics Research and Applications **18**(3): 291-311.

Act, C. (2001). Corporations Act 2001. Commonwealth of Australia. Canberra, ACT, Australian Government.

Adini, B., *et al.* (2017). "Striving to be resilient: What concepts, approaches and practices should be incorporated in resilience management guidelines?" Technological Forecasting and Social Change **121**: 39-49.

Adner, R. and C. E. Helfat (2003). "Corporate effects and dynamic managerial capabilities." Strategic management journal **24**(10): 1011-1025.

AG (2010). Critical infrastructure resilience strategy. A. G. s. Department. Canberra, ACT, Commonwealth of Australia.

AG (2011). Australian Emergency Management Handbook. Canberra, ACT, Commonwealth of Australia.

AG (2015). Critical Infrastructure Resilience Strategy: Plan, Available online at http://www.tisn.gov.au/Documents/CriticalInfrastructureResilienceStrategyPlanAccessible.pdf. Trusted Information Sharing Network (TISN). Canberra, ACT, Attorney-General Department.

AG (2016). Organisational Resilience HealthCheck, Available online at https://www.organisationalresilience.gov.au/HealthCheck/Pages/default.aspx. A. G. s. Department. Canberra, ACT, Commonwealth of Australia.

AG (2017). Strengthening the Security of Australia's Critical Infrastructure C. I. Centre. Canberra, ACT, Commonwealth of Australia.

AG (2018). Emergency response plans, Available online at https://www.ag.gov.au/EmergencyManagement/Emergency-response-plans/Pages/default.aspx. A. General. Canberra, ACT, Australian Government.

AICD (2016). Risk management: Role of the board. Director Tools, Australian Institute of Company Directors.

AIDR (2018). "Australian Disaster Resilience Glossary." The Australian Disaster Resilience Knowledge Hub.

AIIMS (2017). The Australasian Inter-Service Incident Management System: a management system for any emergency. East Melbourne, VIC, Australasian Fire and Emergency Service Authorities Council (AFAC).

Aitsi-Selmi, A., *et al.* (2015). "The Sendai framework for disaster risk reduction: Renewing the global commitment to people's resilience, health, and well-being." International Journal of Disaster Risk Science **6**(2): 164-176.

Alcantara, P., *et al*. (2017). BCI supply chain resilience report. Technical report. Caversham, UK, Business Continuity Institute.

Alcaraz, C. and S. Zeadally (2015). "Critical infrastructure protection: Requirements and challenges for the 21st century." International journal of critical infrastructure protection **8**: 53-66.

Ammann, W. J., *et al.* (2006). RISK21-Coping with Risks Due to Natural Hazards in the 21st Century. RISK21 Workshop, 28 November-3 December 2004, Monte Verità, Ascona, Switzerland, CRC Press.

Alderton, P. (2013). Port Management and Operations. London, UK, Informa.

Alderton, P. and G. Saieva (2013 [2008]). Port management and operations. London, UK, Taylor & Francis.

Alesi, P. (2008). "Building enterprise-wide resilience by integrating business continuity capability into day-to-day business culture and technology." Journal of Business Continuity & Emergency Planning **2**(3): 214-220.

Allen, D. K., *et al.* (2014). "Information sharing and interoperability: the case of major incident management." European Journal of Information Systems **23**(4): 418-432.

Allen, J. T., *et al*. (2014). "Future Australian severe thunderstorm environments. Part II: The influence of a strongly warming climate on convective environments." Journal of Climate **27**(10): 3848-3868.

Alpaslan, C. M., *et al*. (2009). "Corporate governance in the context of crises: Towards a stakeholder theory of crisis management." Journal of Contingencies and Crisis Management **17**(1): 38-49.

Altiok, T. (2011). "Port security/safety, risk analysis, and modelling." Annals of Operations Research **187**(1): 1-3.

AMSA (2017). Intergovernmental agreement on the National Plan to Combat Pollution of the Sea by Oil and other Noxious and Hazardous Substances, Available online at https://www.amsa.gov.au/about-us/who-we-work/intergovernmental-agreement-national-plan-combat-pollution-sea-oil-and-other. Australian Maritime Safety Authority. Canberra, ACT, Australian Government.

AMSA (2018). "National Plan for Maritime Environmental Emergencies: Exercise Westwind 2015 Evaluation Report, Available online at https://www.amsa.gov.au/marine-environment/national-plan-maritime-environmental-emergencies/exercise-westwind-2015." Retrieved 24 March 2018.

Anderson, D. R. (2006). "The critical importance of sustainability risk management." Risk Management **53**(4): 66.

Anderson, T. W. (2003). An Introduction to Multivariate Statistical Analysis. Hoboken, NJ, Wiley.

Andersson, C. and P. Törnberg (2018). "Wickedness and the anatomy of complexity." Futures **95**: 118-138.

Andrews, D., *et al.* (2003). "Conducting research on the internet: Online survey design, development and implementation guidelines." International Journal of Human-Computer Interaction **16**(2): 185-210.

Anton, D. (2017). "Negotiating the Settlement of the Timor Sea Boundary Dispute between Australia and Timor Leste." Asia-Pacific Journal of Ocean Law and Policy **2**.

Antonakis, J. and D. V. Day (2017). The Nature of Leadership. Thousand Oaks, CA, SAGE Publications.

Antwerp, (2015). European handbook of maritime security exercises and drills, Antwerp, Belgium, Antwerp Port Authority**:** 184.

Arouri, M., *et al.* (2015). "Natural disasters, household welfare, and resilience: Evidence from rural Vietnam." World development **70**: 59-77.

Arrow, J. (2012). RISK. 845 Risk Intelligence and Measuring Excellence in Project Risk Management. Morgantown, West Virginia, Association for the Advancement of Cost Engineering (AACE).

Arup (2017). "Port of Melbourne Webb Dock Redevelopment, Available online at https://www.arup.com/projects/port-of-melbourne-webb-dock-redevelopment."

Ary, D., *et al*. (2018). Introduction to Research in Education. US, Cengage Learning.

Assmuth, T., *et al*. (2010). "Integrated risk assessment and risk governance as socio-political phenomena: A synthetic view of the challenges." Science of the Total Environment **408**(18): 3943-3953.

Astle, W. E. (1996). The Safe Port or Berth Reachable on Arrival: Charterers' and Shipowners' Responsibilities and Liabilities. Surrey, UK, Fairplay Publications.

Atlas, R. I. (2013). 21st century security and CPTED: Designing for critical infrastructure protection and crime prevention. Boca Raton, FL, CRC Press.

Austlii (2018). Data bases – Cwlth of Australia. Retrieved 13 March 2018, from https://www.austlii.edu.au/databases.html#.

Aven, T. (2007). "A unified framework for risk and vulnerability analysis covering both safety and security." Reliability Engineering & System Safety **92**(6): 745-754.

Aven, T. (2011). "On risk governance deficits." Safety Science **49**(6): 912-919.

Aven, T. (2015). Risk analysis. Chichester, UK, John Wiley & Sons.

Aven, T. (2016). "Risk assessment and risk management: Review of recent advances on their foundation." European Journal of Operational Research **253**(1): 1-13.

Aven, T. (2017). A conceptual foundation for assessing and managing risk, surprises and black swans. The illusion of risk control: What does it take to live with uncertainty? E. Marsden, C. Kamat and F. Daniellou, Springer**:** 23-39.

Aven, T. and B. S. Krohn (2014). "A new perspective on how to understand, assess and manage risk and the unforeseen." Reliability Engineering & System Safety **121**: 1-10.

Aven, T. and O. Renn (2010). Risk Management and Governance: Concepts, Guidelines and Applications. Heidelberg, Germany, Springer.

Aven, T. and E. Zio (2018). Knowledge in Risk Assessment and Management, John Wiley & Sons.

Ayyub, B. M. and G. J. Klir (2006). Uncertainty Modelling and Analysis for Engineers and Scientists. Boca Raton, Florida, Chapman & Hall/CRC Press.

Ayyub, B. M. (2014). Risk Analysis in Engineering and Economics. Boca Raton, FA, CRC Press.

Bach, C., *et al*. (2013). "Adding value to critical infrastructure research and disaster risk management: the resilience concept, Available online at http://sapiens.revues.org/1626." SAPIENS: Surveys and Perspectives Integrating Environment and Society **6**(1).

Bahadur, A., *et al*. (2015). "Resilience frameworks: a review." London: Overseas Development Institute.

Bahadur, A., *et al.* (2015). "Measuring resilience: An analytical review (draft under review)." Climate and Development.

Bailey, J. and D. Peetz (2014). "Australian unions and collective bargaining in 2013." Journal of Industrial Relations **56**(3): 415-432.

Bak, O. (2018). "Supply chain risk management research agenda: From a literature review to a call for future research directions." Business Process Management Journal **24**(2): 567-588.

Baker-Beall, C., *et al.,* Eds. (2015). Counter-radicalisation: Critical perspectives. Routledge critical terrorism series. Abingdon, UK, Routledge.

Bakker, A. B. and W. B. Schaufeli (2008). "Positive organizational behavior: Engaged employees in flourishing organizations." Journal of Organizational Behavior: The International Journal of Industrial, Occupational and Organizational Psychology and Behavior **29**(2): 147-154.

Banasiewicz, A. D. (2015). "The ecosystem of executive threats: A conceptual overview." Risk Management **17**(2): 109-143.

Bandara, Y. M. and H.-O. Nguyen (2015). "Port infrastructure pricing policy and practice: a case study of Australia and New Zealand seaports." Australian Journal of Maritime & Ocean Affairs **7**(2): 110-131.

Bank, W. (2016). Port Reform Toolkit PPIAF, Available online at https://ppp.worldbank.org/public-private-partnership/library/port-reform-toolkit-ppiaf-world-bank-2nd-edition. Washington, DC, World Bank.

Barlett, J. E., *et al.* (2001). "Organizational research: Determining appropriate sample size in survey research." Information technology, learning, and performance journal **19**(1): 43.

Barnes, P., *et al*. (2015). Chinese investment in the Port of Darwin: A strategic risk for Australia? Strategic Insights. Canberra, ACT, Australian Strategic Policy Institute**:** 1-20.

Barney, J. and T. Felin (2013). "What are microfoundations?" The Academy of Management Perspectives **27**(2): 138-155.

Bartlett, D. and R. Singh (2018). Exploring Natural Hazards: A Case Study Approach. Boca Raton, Florida, CRC Press.

Bazeley, P. (2017). Integrating analyses in mixed methods research. London, UK, Sage.

BCI (2008). A management guide to implementing global good practice in business continuity management. Good practice guidelines. Caversham, UK, Business Continuity Institute.

Beasley, M. S. and M. L. Frigo (2010). ERM and its role in strategic planning and strategy execution. Enterprise Risk Management. J. Fraser and B. J. Simkins. Hoboken, NJ, Wiley.

Beaumont, P. (2017). Cyber-risks in maritime container ports: An analysis of threats and simulation of impacts. Information Security Group Technical Report. Egham, Surrey UK, Royal Holloway University of London**:** 1-71.

Beccari, B. (2016). "A comparative analysis of disaster risk, vulnerability and resilience composite indicators, Available online at https://www.ncbi.nlm.nih.gov/pmc/articles/PMC4807925/." PLoS currents **8**.

Becker, A. and M. R. Caldwell (2015). "Stakeholder perceptions of seaport resilience strategies: a case study of Gulfport (Mississippi) and providence (Rhode Island)." Coastal Management **43**(1): 1-34.

Becker, A., *et al.* (2016). "A method to estimate climate-critical construction materials applied to seaport protection." Global environmental change **40**: 125-136.

Becker, A., *et al*. (2013). A Method and Typology to Assess Impacts of Hurricanes on Seaport Stakeholder Clusters: A Case Study of Gulfport, MS. Engineering Working Paper #WP134, Stanford University Center for Integrated Facility.

Becker, A., *et al*. (2017). "Cost and Materials Required to Retrofit US Seaports in Response to Sea Level Rise: A Thought Exercise for Climate Response." Journal of Marine Science and Engineering **5**(3): 44.

Becker, A., *et al.* (2018). "Implications of climate change for shipping: Ports and supply chains." Wiley Interdisciplinary Reviews: Climate Change **9**(2).

Becker, A. H., *et al*. (2015). "Towards seaport resilience for climate change adaptation: Stakeholder perceptions of hurricane impacts in Gulfport (MS) and Providence (RI)." Progress in Planning **99**: 1-49.

Beins, B. C. and M. A. McCarthy (2012). Research methods and statistics. Upper Saddle River, New Jersey, Pearson Education.

Bekefi, T. and M. J. Epstein (2006). Integrating social and political risk into management decision-making. Management Accounting Guideline. Toronto, Canada, The Society of Management Accountants of Canada, and The American Institute of Certified Public Accountants.

Belluz, D. D. B., *et al*. (2014). Operational risk management. Enterprise Risk Management. J. Fraser, B. J. Simkins and K. Narvaez**:** 279-301.

Béné, C. (2013). "Towards a quantifiable measure of resilience." IDS Working Papers **2013**(434): 1-27.

Beresford, A. K. C., *et al*. (2004). "The UNCTAD and WORKPORT Models of Port Development: Evolution or Revolution?" Maritime Policy & Management: The flagship journal of international shipping and port research **31**(2).

Bergtold, J. S., *et al*. (2015). On the Examination of the Reliability of Statistical Software for Estimating Logistic Regression Models. 2015 AAEA & WAEA Joint Annual Meeting, July 26-28, San Francisco, California, Agricultural and Applied Economics Association & Western Agricultural Economics Association.

Berkes, F. (2017). "Environmental Governance for the Anthropocene? Social-Ecological Systems, Resilience, and Collaborative Learning." Sustainability **9**(7): 1232.

Berkes, F. and H. Ross (2013). "Community resilience: toward an integrated approach." Society & Natural Resources **26**(1): 5-20.

Berle, Ø. (2012). Risk and Resilience in Global Maritime Supply Chains. Department of Petroleum Engineering. Trondheim, Norway, Norwegian University of Science and Technology. PhD Thesis**:** 177.

Berle, Ø., *et al.* (2011a). "Formal vulnerability assessment of a maritime transportation system." Reliability Engineering & System Safety **96**(6): 696-705.

Berle, Ø., *et al.* (2011b). "Failure modes in the maritime transportation system: A functional approach to throughput vulnerability." Maritime Policy & Management **38**(6): 605-632.

Bernstein, P. L. (1998). Against the Gods: the remarkable story of Risk. John Wiley& Sons. New York, NY, John Wiley.

Beroggi, G. and W. A. Wallace (2012). Operational risk management: The integration of decision, communications, and multimedia technologies. New York, NY, Springer Science & Business Media.

Berthod, O., *et al.* (2017). "From high-reliability organizations to high-reliability networks: the dynamics of network governance in the face of emergency." Journal of Public Administration Research and Theory **27**(2): 352-371.

Best, J. W. and J. V. Kahn (2006). Research in education / - 10th ed. Boston, MA, Pearson.

Bethlehem, J. and S. Biffignandi (2012). Handbook of web surveys. Hoboken, NJ, Wiley.

Bhamra, R. (2018). Manufacturing and supply chain dynamic capabilities for resilience. Post graduate research project. Leicestershire, UK, Loughborough University.

Bhandari, R. B., *et al*. (2015). "Incident management approaches above the Incident Management Team level in Australia." Journal of Homeland Security and Emergency Management **12**(1): 101-119.

Bichou, K. (2018). Port Operations, Planning and Logistics. Abingdon, UK, Routledge.

Bichou, K., *et al*. (2014). Risk Management in Port Operations, Logistics and Supply Chain Security. Abingdon, UK, Routledge.

Bichou, K. and R. Gray (2004). "A Logistics and Supply Chain Management Approach to Port Performance Measurement." Maritime Policy and Management **31**: 47-67.

Bichou, K. and R. Gray (2005). A Logistics and Supply Chain Approach to Seaport Efficiency - An Inquiry Based on Action Research Methodology Research Methodologies in Supply Chain Management. H. Kotzab, S. Seuring, M. Müller and G. Reiner. Heidelberg, Germany, Physica-Verlag**:** 413 - 428.

Biener, C., *et al*. (2015). "Insurability of cyber risk: An empirical analysis." The Geneva Papers on Risk and Insurance-Issues and Practice **40**(1): 131-158.

Biffignandi, S. and J. Bethlehem (2012). Web surveys: methodological problems and research perspectives. Advanced Statistical Methods for the Analysis of Large Data-Sets. D. C. A., C. M. and A. I. J. Berlin, Heidelberg, Springer**:** 363-373.

Bigley, G. A. and K. H. Roberts (2001). "The incident command system: High-reliability organizing for complex and volatile task environments." Academy of Management Journal **44**(6): 1281-1299.

Bird, L. (2011). Dictionary of business continuity management terms. Caversham, UK, Business Continuity Institute.

Birkland, T. A. and M. K. Warnement (2017). Focusing events, risk, and regulation. Policy Shock: Recalibrating Risk and Regulation after Oil Spills, Nuclear Accidents and Financial Crises. E. J. Balleisen, L. S. Bennear, K. D. Krawiec and J. B. Wiener. Cambridge, UK, Cambridge University Press**:** 107.

Birrell, M. (2016). Port of Melbourne Corporation 2015-16 Annual Report. Melbourne, Victoria, Port of Melbourne Corporation.

Bititci, U., *et al.* (2012). "Performance measurement: challenges for tomorrow." International Journal of Management Reviews **14**(3): 305-327.

Bititci, U. S. (2015). Managing business performance: The science and the art. Chichester, UK, John Wiley & Sons.

Bititci, U. S., *et al*. (1997). "Integrated performance measurement systems: a development guide." International journal of operations & production management **17**(5): 522-534.

Bititci, U. S., *et al*. (2015). "Value of maturity models in performance measurement." International Journal of Production Research **53**(10): 3062-3085.

BITRE (2017). Australian sea freight 2014-15, available online at https://bitre.gov.au/publications/2017/files/asf_2014_15.pdf. Canberra, ACT, Bureau of Infrastructure, Transport and Regional Economics (BITRE)

Black, J., *et al*. (2018). "Issues in Dry Port Location and Implementation in Metropolitan Areas: The Case of Sydney, Australia." Transactions on maritime science **7**(01): 41-50.

Blades, A. (2017). "Organisational resilience: What does it mean?" Governance Directions **69**(11): 669.

Blaikie, P., *et al*. (2014). At risk: natural hazards, people's vulnerability and disasters. Abingdon, UK, Routledge.

Blecker, T., *et al*. (2008). Management in Logistics Networks and Nodes: Concepts, Technology and Applications. Berlin, Germany, Erich Schmidt Verlag GmbH & Co KG.

Boin, A. (2004). "Lessons from crisis research." International studies review **6**(1): 165-174.

Boin, A., *et al.* (2010). The rise of resilience. Designing resilience: Preparing for extreme events. L. K. Comfort, A. Boin and C. C. Demchak. Pittsburgh, PA, University of Pittsburgh Press**:** 1-12.

Boin, A., *et al*. (2017). The politics of crisis management: Understanding public leadership when it matters most. Cambridge, UK, Cambridge University Press.

BOM (2016). How does Australia's tsunami warning system work? Available online at http://media.bom.gov.au/social/blog/1062/how-does-australias-tsunami-warning-system-work/. B. o. Meteorology. Melbourne, VIC, Australian Government.

BOM (2018). Annual climate statement 2017. Melbourne, VIC, Bureau of Meteorology.

Bond, A., *et al.* (2015). "Managing uncertainty, ambiguity and ignorance in impact assessment by embedding evolutionary resilience, participatory modelling and adaptive management." Journal of environmental management **151**: 97-104.

Boone, H. N. and D. A. Boone (2012). "Analyzing Likert data." Journal of extension **50**(2): 1-5.

Booth, S. A. (2015). Crisis management strategy: Competition and change in modern enterprises. Abingdon, UK, Routledge.

Borgonovo, E. (2017). Uncertainty Quantification. Sensitivity Analysis. Cham, Switzerland, Springer**:** 117-127.

Borgonovo, E., *et al.* (2018). "Risk analysis and decision theory: A bridge." European Journal of Operational Research **264**(1): 280-293.

Borum, R. (2007). Psychology of terrorism. Mental Health Law & Policy Faculty Publications. Tampa, FLA, University of South Florida.

Borum, R. and T. Neer (2017). Terrorism and Violent Extremism. Handbook of Behavioral Criminology. V. B. Van Hasselt and M. L. Bourke. Cham, Switzerland, Springer International Publishing**:** 729-745.

Borys, S. (2018). Russian hacking: Up to 400 Australian companies caught up in cyber-attacks blamed on Moscow, Available online at http://www.abc.net.au/news/2018-04-17/australians-caught-up-in-cyber-attacks-blamed-on-russia/9665820. ABC News.

Bosnjak, M. and T. L. Tuten (2001). "Classifying response behaviors in web-based surveys." Journal of Computer-Mediated Communication **6**(3): JCMC636.

Bottasso, A., *et al.* (2014). "Ports and regional development: a spatial analysis on a panel of European regions." Transportation research part A: policy and practice **65**: 44-55.

Bouvard, M. and S. Lee (2016). Risk management failures, Available online at https://ssrn.com/abstract=2614468 or http://dx.doi.org/10.2139/ssrn.2614468 Finance Working Paper European Corporate Governance Institute (ECGI).

Bower-White, G. (2012). Demonstrating adequate management of risks: the move from quantitative to qualitative risk assessments. SPE Asia Pacific Oil and Gas Conference and Exhibition, Perth, Australia Society of Petroleum Engineers.

Brace, I. (2018). Questionnaire design: How to plan, structure and write survey material for effective market research. London, UK, Kogan Page Publishers.

Bralver, C. N. and D. Borge (2010). Managing increased capital markets intensity. The Known, the Unknown, and the Unknowable in Financial Risk Management: Measurement and Theory Advancing Practice. F. X. Diebold, N. A. Doherty and R. J. Herring. Princeton, US, Princeton University Press.

Bram, S., *et al.* (2016). Decision-making and human behavior in emergencies with cascading effects. CascEff Deliverable D. Lorraine, France, University of Lorraine. **3**.

Branch, A. and M. Stopford (2013). Maritime economics. Abingdon, UK, Routledge.

Brand, F. (2009). Resilience and sustainable development: an ecological inquiry. München, Germany, Technische Universität München. PhD Thesis

Brannen, J. (2017). Mixing methods: Qualitative and quantitative research. Abingdon, UK, Routledge.

Brasington, H. and M. Park (2016). Cybersecurity and ports: Vulnerabilities, consequences and preparation. Ausmarine. Melbourne, Vic, Baird Publication. **February 2016**.

Brasington, H. and M. Park (2016). "Cybersecurity and ports: Vulnerabilities, consequences and preparation." Ausmarine **38**(4): 23.

Breuer, C., *et al.* (2013). "Collaborative Risk Management in Sensitive Logistics Nodes." Team Performance Management **19**(7/8): 331-351.

Bridges, G. E. (2004). Illustrative Development Scenarios, Available online at http://www.royalroads.ca/NR/rdonlyres/FC9E3EA6-5EF1-40E9-A488-67D28046C998/0/tab_2_illustrative_scenario.pdf British Columbia Offshore Oil and Gas Socio-Economic Issue Papers. Victoria, British Columbia, Royal Roads University**:** 35.

Brindley, C. (2017). Supply Chain Risk. Abingdon, UK, Taylor & Francis.

Briske, D. D., *et al.* (2006). "A unified framework for assessment and application of ecological thresholds." Rangeland Ecology & Management **59**(3): 225-236.

Briske, D. D., *et al.* (2017). Nonequilibrium ecology and resilience theory. Rangeland Systems, Springer**:** 197-227.

Bristow, G. and A. Healy (2014). "Regional resilience: an agency perspective." Regional studies **48**(5): 923-935.

Brodsky, A. E., *et al.* (2011). "Between synergy and conflict: Balancing the processes of organizational and individual resilience in an Afghan women's community." American journal of community psychology **47**(3-4): 217-235.

Bromiley, P., *et al.* (2015). "Enterprise risk management: Review, critique, and research directions." Long range planning **48**(4): 265-276.

Brooks, B., *et al.* (2018). "Human error during the multilevel responses to three Australian bushfire disasters." Journal of Contingencies and Crisis Management: 1-13.

Brooks, M. R., *et al.* (2017). "Revisiting port governance and port reform: A multi-country examination." Research in Transportation Business & Management **22**: 1-10.

Brown, C., *et al.* (2017). "Measuring the organizational resilience of critical infrastructure providers: A New Zealand case study." International journal of critical infrastructure protection **18**: 37-49.

Bruneau, M., *et al.* (2003). "A framework to quantitatively assess and enhance the seismic resilience of communities." Earthquake spectra **19**(4): 733-752.

Brustbauer, J. (2016). "Enterprise risk management in SMEs: Towards a structural model." International Small Business Journal **34**(1): 70-85.

Bryman, A. (2015). Social research methods. Oxford, UK, Oxford University Press.

Bryman, A. and E. Bell (2015). Business Research Methods. Oxford, UK, Oxford University Press.

Brynjolfsson, E. and A. McAfee (2014). The second machine age: Work, progress, and prosperity in a time of brilliant technologies. New York, NY, WW Norton & Company.

BSI (2011). BS 31100:2011 Risk management – Code of practice and guidance for the implementation of BS ISO 31000. London, UK, British Standards Institution.

BSI (2014). BS 65000 Guidance for Organizational Resilience. London, UK, British Standards Institution.

Bugalla, J. and K. Narvaez (2014). The Perils of Silos in Risk Management, Available online at http://ww2.cfo.com/accounting-tax/2014/05/the-perils-of-silos-in-risk-management/. CFO Magazine. New York, NY, Argyle Executive Forum.

Burnard, K. and R. Bhamra (2011). "Organisational resilience: development of a conceptual framework for organisational responses." International Journal of Production Research **49**(18): 5581-5599.

Burnard, K., *et al.* (2018). "Building organisational resilience: four configurations." IEEE transactions on engineering management.

Burns, M. G. (2015). Port Management and Operations. Boca Raton, US, CRC Press.

Burns, T. and G. M. Stalker (1994). The Management of Innovation. Oxford, UK, Oxford University Press.

Butterfield, B. P. (2017). Traditional risk management vs enterprise risk management: Which approach is the best choice for your company? Orlando, FL, Lowndes, Drosdick, Doster, Kantor & Reed.

Cahoon, S., *et al.* (2015). "The impact of climate change on Australian ports and supply chains." Climate Change and Adaptation Planning for Ports: 194.

Cahoon, S., *et al.* (2016). The impact of climate change on Australian ports and supply chains: the emergence of adaptation strategies. Climate Change and Adaptation Planning for Ports. A. K. Y. Ng, A. Becker, S. Cahoon *et al.* Abingdon, UK, Routledge.

Cahoon, S. C. (2004). Seaport Marketing: A Census of Australian Seaports, University of Tasmania. PhD Thesis**:** 255.

Caldwell, S. L. (2017). Cybersecurity: Wake-up call. The Maritime Executive. Fort Lauderdale, FLA, The Maritime Executive. **21:** 70-79.

Callegaro, M., *et al.* (2015). Web survey methodology. London, UK, Sage.

Capineri, C. and F. Randelli (2007). "Freight Transportation Flows: New Trade Regions and Trade Routes." European Journal of Transport and Infrastructure Research **7**(2): 93-112.

Caralli, R. A. (2006). Sustaining Operational Resiliency: A Process Improvement Approach to Security Management. Technical Note CMU/SEI-2006-TN-009. Pittsburgh, PA Carnegie Mellon University.

Caralli, R. A., *et al.* (2010). CERT ® Resilience Management Model, Version 1.0. Improving Operational Resilience Processes. Pittsburgh, PA, US, Software Engineering Institute, Carnegie Mellon University.

Caralli, R. A., *et al.* (2012). Maturity models 101: A primer for applying maturity models to smart grid security, resilience, and interoperability. Pittsburgh, PA, Carnegie-Mellon University - Software Engineering Institute.

Cardona, O-D., *et al.* (2012). Determinants of risk: exposure and vulnerability. Managing the Risks of Extreme Events and Disasters to Advance Climate Change Adaptation. C. B. Field, V. Barros, T. F. Stocker *et al.* Cambridge, UK, Cambridge University Press 65-108.

Carr, M. (2016). "Public–private partnerships in national cyber-security strategies." International Affairs **92**(1): 43-62.

Carvalho, M., *et al.* (2012). Organic Resilience for Tactical Environments. 5th International ICST Conference, BIONETICS 2010. J. Suzuki and T. Nakano. Boston, USA, Springer 22-29.

Casal, J. (2017). Evaluation of the effects and consequences of major accidents in industrial plants. Amsterdam, The Netherlands, Elsevier.

Caselli, F., *et al.* (2016). "Methodology and procedure of business impact analysis for improving port logistics business continuity management." IDRiM Journal **6**(1): 1-29.

Cavaliere, R. (2015). "How to choose the right statistical software? — a method increasing the post-purchase satisfaction." Journal of thoracic disease **7**(12): E585.

Cavallo, A. (2014). "Integrating disaster preparedness and resilience: a complex approach using System of Systems." Australian Journal of Emergency Management, The **29**(3): 46.

Cavusgil, S. T., *et al.* (2014). International business: The new realities. Melbourne, VIC, Pearson Australia.

Cetin, C. K. and G. Cerit (2010). "Organizational Effectiveness at Seaports: A Systems Approach." Maritime Policy & Management: The flagship journal of international shipping and port research **37**(3): 195-219.

Chacon, N., *et al.* (2012). New Models for Addressing Supply Chain and Transport Risk. Supply Chain and Transport Risk Initiative M. Stafaner and A. Wright. Geneva, Switzerland, World Economic Forum.

Chaffin, B. C., *et al.* (2014). "A decade of adaptive governance scholarship: synthesis and future directions." Ecology and Society **19**(3).

Chandler, D. (2014). Resilience: The governance of complexity. Abingdon, UK, Routledge.

Chandler, D. and J. Coaffee (2016). The Routledge Handbook of International Resilience, Taylor & Francis.

Chapman, R. (2011). Simple tools and techniques for enterprise risk management. Chichester, UK, John Wiley.

Charmaz, K. (2006). Constructing grounded theory: A practical guide through qualitative analysis London, UK, Sage.

Chen, P. S.-L., *et al.* (2017). "The latest trend in Australian port privatisation: Drivers, processes and impacts." Research in Transportation Business & Management **22**: 201-213.

Chen, S.-L. and S. Everett (2014). "The dynamics of port reform: different contexts, similar strategies." Maritime Policy & Management **41**(3): 288-301.

Chen, X. (2016). "System vulnerability assessment and critical nodes identification." Expert Systems with Applications **65**: 212-220.

Chernov, D. and D. Sornette, Eds. (2016). Man-made Catastrophes and Risk Information Concealment: Case Studies of Major Disasters and Human Fallibility. Heidelberg, Germany, Springer.

Chhetri, P., *et al.* (2015). "Seaport resilience to climate change: Mapping vulnerability to sea-level rise." Journal of Spatial Science **60**(1): 65-78.

Chhetri, P., *et al.* (2013). Functional resilience of port environs in a changing climate - assets and operations. Work Package 2 of Enhancing the resilience of seaports to a changing climate report series. Gold Coast, Australia, National Climate Change Adaptation Research Facility. **2**.

Chong, D. G. S. (1992). "Revisiting the Safe Port." Singapore Journal of Legal Studies **79**: 79-114.

Choy, K. L., *et al.* (2007). "Managing Uncertainty in Logistics Service Supply Chain." International Journal of Risk Assessment and Management **7**(1): 19-43.

Christensen, L. A., *et al.* (2015). Research Methods, Design, and Analysis. Harlow, UK, Pearson Education Limited.

Christensen, T., *et al.* (2016). "Organizing for crisis management: Building governance capacity and legitimacy." Public Administration Review **76**(6): 887-897.

Christopher, M. (2010). New Directions in Logistics Global Logistics: New Directions in Supply Chain Management. C. D. J. Waters. London, UK Kogan Page.

Christopher, M. (2016). Logistics & supply chain management. Harlow, UK, Pearson Higher Education.

Christopher, M. and M. Holweg (2017). "Supply chain 2.0 revisited: A framework for managing volatility-induced risk in the supply chain." International Journal of Physical Distribution & Logistics Management **47**(1): 2-17.

Church, A. H. and J. Waclawski (2017). Designing and using organizational surveys. London, UK, Routledge.

Clark, I. (2016). Business continuity management. The Risk Management Handbook: A Practical Guide to Managing the Multiple Dimensions of Risk. D. Hillson. London, UK, Kogan Page.

Clark, L. A. and D. Watson (1995). "Constructing validity: Basic issues in objective scale development." Psychological assessment **7**(3): 309.

Clark, R. M. and S. Hakim (2017). Protecting critical infrastructure at the state, provincial, and local level: Issues in cyber-physical security. Cyber-physical security. Protecting critical infrastructure. C. R. M. and H. S. Cham, Switzerland, Springer. **3:** 1-17.

Coaffee, J. and J. Clarke (2016). Resilience and Risk: Realising Critical Infrastructure Resilience. NATO Advanced Research Workshop on Resilience-Based Approaches to Critical Infrastructure Safeguarding, 26–29 June Azores, Portugal, Springer.

Coaffee, J. and J. Clarke (2017). "Critical infrastructure lifelines and the politics of anthropocentric resilience." Resilience **5**(3): 161-181.

Cochran, W. G. (1977). Sampling techniques. New York, John Wiley & Sons.

Cockram, D. and C. Van den Heuvel (2012). Organisational resilience. Caversham, Berkshire UK, Business Continuity Institute.

Cohen, L., *et al.* (2013). Research methods in education. London, UK, Routledge.

Cole, M. A., *et al.* (2013). Natural Disasters and Plant Survival: The Impact of the Kobe Earthquake Studies on the Structure of Japanese Economic Space and Japanese Supply Chains Sustaining Growth Under Globalization and Disaster Risks. Tokyo, Japan, Research Institute of Economy, Trade and Industry (RIETI).

Coleman, L. (2004). "The frequency and cost of corporate crises." Journal of Contingencies and Crisis Management **12**(1): 2-13.

Collier, S. J. (2008). "Enacting catastrophe: preparedness, insurance, budgetary rationalization." Economy and society **37**(2): 224-250.

Colyvan, M., *et al.* (2017). Addressing Risk in Conditions of Uncertainty, Ignorance, and Partial Knowledge. Canberra, ACT, Academy of Science

Conklin, J. (2006). Wicked problems & social complexity, CogNexus Institute.

Connell, S. D. and G. Ghedini (2015). "Resisting regime-shifts: The stabilising effect of compensatory processes." Trends in ecology & evolution **30**(9): 513-515.

Connor, L. H. (2012). "Experimental publics: Activist culture and political intelligibility of climate change action in the Hunter Valley, Southeast Australia." Oceania **82**(3): 228-249.

Constas, M. and C. Barrett (2013). Principles of Resilience Measurement for Food Security: Metrics, Mechanisms, and Implementation Issues. Expert Consultation on Resilience Measurement Related to Food Security Rome, Food and Agricultural Organisation and World Food Program (FAO).

Cosco, T. D., *et al.* (2016). "Operationalising resilience in longitudinal studies: a systematic review of methodological approaches." Journal of Epidemiology and Community Health Published Online**.**

COSO (2004). Enterprise risk management: integrated framework. Jersey City, NJ, Committee of Sponsoring Organizations of Treadway Commission.

Couper, M. P. and P. V. Miller (2008). "Web survey methods: Introduction." Public Opinion Quarterly **72**(5): 831-835.

Cova, T. J. and S. M. Conger (2004). Transportation Hazards. Handbook of Transportation Engineering M. Kutz. New York, McGraw-Hill**:** 17.11-17.24.

Covello, V. T. and J. Mumpower (1985). "Risk analysis and risk management: an historical perspective." Risk analysis **5**(2): 103-120.

Craighead, C. W., *et al.* (2007). "The Severity of Supply Chain Disruptions: Design Characteristics and Mitigation Capabilities." Decision Sciences **38**(1): 131-156.

Crawford, L., *et al.* (2012). Building capability for disaster resilience. 28th Annual Conference of Association of Researchers in Construction Management (ARCOM), Sep. 2012. Edinburgh, Scotland, Bond University, Institute of Sustainable Development and Architecture

Creswell, J. (2009). Research Design: Qualitative, Quantitative and Mixed Methods Approaches. Los Angeles, US, Sage.

Creswell, J. W. (2010). Mapping the developing landscape of mixed methods research. Los Angeles, CA, Sage.

Creswell, J. W. (2014). A concise introduction to mixed methods research. Thousand Oaks, CA, Sage Publications.

Creswell, J. W. and J. D. Creswell (2017). Research design: Qualitative, quantitative, and mixed methods approaches. Thousand Oaks, CA, Sage publications.

Creswell, J. W. and V. L. Plano Clark (2011). Designing and conducting mixed methods research. Los Angeles, CA, Sage Publications.

Cretney, R. (2014). "Resilience for Whom? Emerging Critical Geographies of Socio-ecological Resilience." Geography Compass **8**(9): 627-640.

Crist, P. (2003). Security in Maritime Transport: Risk Factors and Economic Impact Paris, France, OECD Directorate for Science, Technology and Industry - Maritime Transport Committee.

Cronstedt, M. (2002). "Prevention, preparedness, response, recovery-an outdated concept?" Australian Journal of Emergency Management, The **17**(2): 10.

Crosby, P. B. (1980). Quality is free: the art of making quality certain. New York, NY, Penguin.

Crowther, D. and S. Sefi (2010). Corporate governance and risk management. Telluride, Colorado, Ventus Publishing.

Crowther, K. G. (2014). "Understanding and overcoming information sharing failures." Journal of Homeland Security and Emergency Management **11**(1): 131-154.

CSIRO (2017). Extreme events, Available online at https://www.csiro.au/en/Research/Environment/Extreme-Events. Canberra, ACT, Commonwealth Scientific and Industrial Research Organisation (CSIRO).

Culley, M. (2017). Resources and Energy Quarterly. D. Thurtell. Canberra, ACT, Department of Industry, Innovation and Science.

Culley, M. (2018). Iron Ore. Resources and Energy Quarterly. D. Thurtell. Canberra, ACT, Department of Industry, Innovation and Science.

Cumming, G. S., *et al.* (2005). "An Exploratory Framework for the Empirical Measurement of Resilience." Ecosystems **8**: 975-987.

Curtin, R., *et al.* (2005). "Changes in telephone survey nonresponse over the past quarter century." Public Opinion Quarterly **69**(1): 87-98.

Curtis, B. (2017). Channel optimisation and risk management through technology at the world's largest bulk export port. Australasian Coasts & Ports 2017: Working with Nature, 21-23 June Cairns, Engineers Australia**:** 310-315.

Cutter, S. L. (2015). Developing a framework for measuring community resilience. Summary of a workshop: Resilient America roundtable. Washington, DC, National Research Council.

Cutter, S. L. (2016). "The landscape of disaster resilience indicators in the USA." Natural Hazards **80**(2): 741-758.

Dahlberg, R., *et al.* (2016). Disaster Research: Multidisciplinary and International Perspectives. Abingdon, UK, Taylor & Francis.

Dahlstrom, N., *et al.* (2009). "Fidelity and validity of simulator training." Theoretical Issues in Ergonomics Science **10**(4): 305-314.

Dahms, T. (2008). Risk Management and Corporate Governance: Are they the same? Risk Management. New York, NY, Risk Management Society. **48:** 10-11.

Dahms, T. (2010). "Resilience and Risk Management, Available online at https://search.informit.com.au/documentSummary;dn=084576038154990;res=IELAPA." Australian Journal of Emergency Management, The **25**(2): 21-26.

Dakos, V., *et al.* (2015). "Resilience indicators: prospects and limitations for early warnings of regime shifts." Philosophical Transactions of the Royal Society B: Biological Sciences **370**(1659): 20130263.

Darbra, R. M. and J. Casal (2004). "Historical Analysis of Accidents in Seaports." Safety Science **42**: 85-98.

Dauvergne, P. and G. LeBaron (2014). Protest Inc.: The corporatization of activism, John Wiley & Sons.

Davidson, H. (2016). Dozens arrested as anti-fossil fuel protesters join Australian coal blockade The Guardian. Sydney, NSW, Guardian News & Media.

Davidson, J., *et al.* (2016). "Interrogating resilience: toward a typology to improve its operationalization." Ecology and Society **21**(2).

Dawson, C. (2010). Introduction to Research Methods: A practical guide for anyone undertaking a research project. London, UK, Constable & Robinson.

De Langen, P. W. and C. Heij (2014). "Corporatisation and performance: A literature review and an analysis of the performance effects of the corporatisation of port of Rotterdam authority." Transport Reviews **34**(3): 396-414.

De Marchi, B. (2015). Risk governance and the integration of different types of knowledge. mo. U. F. Paleo. Dordrecht, The Netherlands, Springer**:** 149-165.

De Martino, M., *et al.* (2013). "Logistics innovation in seaports: An inter-organizational perspective." Research in Transportation Business & Management **8**: 123-133.

De Martino, M., *et al.* (2010). Value Creation within Port Supply Network: Methodological Issues. 26th IMP Conference, 2-4 September Budapest, Hungary.

de Vaus, D. (2014). Surveys in social research. Sydney, NSW, Allen & Unwin.

Decaux, L. (2015). Internal auditing and organizational governance: the combined assurance approach. Louvain School of Management. Brussels, Belgium, Université Catholique de Louvain. PhD Thesis.

Dekker, S., *et al.* (2016). Crew resilience and simulator training in aviation. Resilience Engineering Perspectives, Volume 1. E. Hollnagel, C. P. Nemeth and S. Dekker. Aldershot, UK, CRC Press**:** 133-140.

Delogu, B. (2016). Risk Analysis and Governance in EU Policy Making and Regulation. Cham, Switzerland, Springer.

Denscombe, M. (2014). The good research guide: for small-scale social research projects. Maidenhead, UK, McGraw-Hill Education (UK).

DeVellis, R. F. (2016). Scale development: Theory and applications. Los Angeles, CA, Sage publications.

Dewey, J. (1938). Logic: The Theory of Inquiry. New York, NY, Holt, Rinehart and Winston.

DFAT (2017). Composition of Trade - Australia 2016-17, Available online at http://dfat.gov.au/about-us/publications/Documents/cot-2016-17.pdf. D. o. F. A. a. Trade. Canberra, ACT, Commonwealth of Australia.

Di Vaio, A. and L. Varriale (2018). "Management innovation for environmental sustainability in seaports: Managerial accounting instruments and training for competitive green ports beyond the regulations." Sustainability **10**(3): 783.

Dias, A. (2017). "A more effective audit after COSO ERM 2017 or after ISO 31000: 2009?" Revista Perspectiva Empresarial **4**(2): 73-82.

Diebold, F. X., *et al.* (2010). The known, the unknown, and the unknowable in financial risk management: measurement and theory advancing practice. Princeton, NJ, Princeton University Press.

Dillman, D. A., *et al.* (2014). Internet, phone, mail, and mixed-mode surveys: the tailored design method. Hoboken, NJ, John Wiley & Sons.

Dingledey, P. M. (2017). Port Automation and Cybersecurity Risks, Available online at http://cimsec.org/port-automation-and-cyber-risk-in-the-shipping-industry/35044 Cimsec. Washington, DC, Center for International Maritime Security.

Dinwoodie, J., *et al.* (2012). Assessing the environmental impact of maritime operations in ports: A systems approach. Maritime Logistics:

Contemporary Issues. D.-W. Song and P. M. Panayides. Bingley, UK, Emerald Group Publishing Limited**:** 263-284.

DiRenzo, J., *et al.* (2015). The little-known challenge of maritime cyber security. 6th International Conference on Information, Intelligence, Systems and Applications (IISA), Corfu, Greece, IEEE.

Doerfel, M. L. and I. Prezelj (2017). "Resilience in a complex and unpredictable world." Journal of Contingencies and Crisis Management **25**(3): 118-122.

Dolgui, A., *et al.* (2017). "Ripple effect in the supply chain: an analysis and recent literature." International Journal of Production Research: 1-17.

Donahue, J. D. and M. H. Moore, Eds. (2012). Ports in a Storm: Public Management in a Turbulent World. Washington, DC, US, Brookings Institution Press.

Doorn, N. (2017). "Resilience indicators: opportunities for including distributive justice concerns in disaster management." Journal of Risk Research **20**(6): 711-731.

Dorfman, M. S. and D. Cather (2012). Introduction to risk management and insurance. Upper Saddle River, N.J. Prentice Hall.

DoT-WA (1999). Port Authorities Act 1999. W. A. Department of Transport. Perth, Western Australia Government.

DoT-WA (2017). Ports Governance Review, Available online at https://www.transport.wa.gov.au/Freight-Ports/ports-governance-review.asp. W. A. Department of Transport. Perth, Western Australia Government.

DoT-WA (2018). Port Authority Boards: Director's Handbook, Available online at https://www.transport.wa.gov.au/Freight-Ports/port-authorities.asp. W. A. Department of Transport. Perth, Western Australia Government.

DoT-WA (2015). Oil Spill Contingency Plan 2015. W. A. Department of Transport. Perth, Western Australia Government.

Downing, T., *et al.* (2002). Climate, Change and Risk. London, UK, Routledge.

Doyle, J. C. (2011). Architecture and Robust Networks. Pasadena, California US California Institute of Technology.

Driscoll, D. L., *et al.* (2007). "Merging qualitative and quantitative data in mixed methods research: How to and why not." Ecological and Environmental Anthropology (University of Georgia) **3**(1): 18-28.

Du Plessis, J. J., *et al.* (2018). Principles of contemporary corporate governance. Cambridge, UK, Cambridge University Press.

Ducruet, C. and T. Notteboom (2012). Developing Liner Service Networks in Container Shipping. Maritime Logistics: A Complete Guide to Effective Shipping and Port Management. D. W. Song and P. Panayides. London, UK, Kogan Page**:** 77-100.

Dueñas-Osorio, L. and S. V. Vemuru (2009). "Cascading Failures in Complex Infrastructure Systems." Structural Safety **31**: 157-167.

Duit, A., *et al.* (2010). "Governance, complexity, and resilience." Global environmental change **20**: 363–368.

Dunn Cavelty, M. and M. l. Suter (2008). "Early warning for critical infrastructure protection and the road to public-private information sharing." Intelligencia y Seguridad **4**: 85-113.

Dunn, T. J., *et al.* (2014). "From alpha to omega: A practical solution to the pervasive problem of internal consistency estimation." British Journal of Psychology **105**(3): 399-412.

Ebbesson, J. (2010). "The rule of law in governance of complex socio-ecological changes." Global environmental change **20**(3): 414-422.

Eggleston, A. (2012). Procurement Procedures for Defence Capital Projects. Foreign Affairs, Defence and Trade References Committee. Parliament House, Canberra, Senate Printing Unit.

EIU (2015). Organisational resilience: Building an enduring enterprise. V. Tuomista. London, UK, The Economist Intelligence Unit.

Elsner, J. B., *et al.* (2008). "The increasing intensity of the strongest tropical cyclones." Nature **455**(7209): 92.

EMA (1998). Australian Emergency Management Glossary - Manual 3. Canberra, Australia, Emergency Management Australia.

EMA (2004). Manual 43 Emergency Planning. E. M. Australia. Canberra, ACT, Commonwealth of Australia.

Ertuğ, Z. K. and N. Girginer (2014). "A Multi Criteria Approach for Statistical Software Selection in Education." Hacettepe Üniversitesi Journal of Education **29**(29-2).

Evans, N. (2015). Pilbara port dividend bonanza. The West Australian. Perth, WA, Seven West Media.

Everett, S. (2003a). "Corporatization: A Legislative Framework for Port Inefficiencies." Maritime Policy & Management: The flagship journal of international shipping and port research **30**(3): 211-219.

Everett, S. (2003b). "Effective Corporatisation Legislation: The Fundamental Issue in Port Management " Australian Journal of Public Administration **62**(3): 26-31.

Everett, S. (2007). "Port reform in Australia: regulation constraints on efficiency." Maritime Policy & Management **34**(2): 107-119.

Eversole, R. (2016). Regional Australia: Being regional. Abingdon, UK, Routledge.

Farjoun, M. (2010). "Beyond dualism: Stability and change as a duality." Academy of Management Review **35**(2): 202-225.

Faulkner, P., *et al.* (2017). "Unknowns, Black Swans and the risk/uncertainty distinction." Cambridge Journal of Economics **41**(5): 1279-1302.

Fenwick, T., *et al.* (2009). Reducing the impact of organisational silos on resilience: a report on the impact of silos on resilience and how the impacts might be reduced. Resilient Organisations Research Report – 2009/01. Christchurch, NZ, Resilient Organisations Research Programme.

Fernández, E. C. (2007). Practical Recommendations to Enable Organisational Reconfigurability from a Complex Systems Perspective. XVII Congreso ACEDE: Flexibilidad y Cambio ante un Nuevo Escenario Competitivo, 16-18 September 2007. Seville, Spain.

Ferretti, M. and F. Schiavone (2016). "Internet of Things and business processes redesign in seaports: The case of Hamburg." Business Process Management Journal **22**(2): 271-284.

Fiksel, J. (2015). Organizational Resilience. Resilient by Design, Springer**:** 129-147.

Fisher, L. (2011). Crashes, Crises, and Calamities: How We Can Use Science to Read the Early-Warning Signs. New York, US, Basic Books.

Fisher, L. (2013). Preparing for Future Catastrophes: Governance Principles for Slow-developing Risks that may have Potentially Catastrophic Consequences. Concept Note, available online at http://www.irgc.org/risk-governance/preparing-for-future-catastrophes/. Lausanne, Switzerland, International Risk Governance Council.

Flage, R. and T. Aven (2015). "Emerging risk–Conceptual definition and a relation to black swan type of events." Reliability Engineering & System Safety **144**: 61-67.

Fleming, C. and M. Bowden (2009). "The most commonly cited disadvantages of web-based surveys are sample frame and non-response bias." Journal of environmental management **90**(1): 284-292.

Fleming, K., *et al.* (2014). The New Multi-HAzard and MulTi-RIsK Assessment MethodS for Europe (MATRIX) Project-An overview of its major findings. EGU General Assembly Conference, 27 April - 2 May, Vienna, Austria, SAO/NASA Astrophysics Data System.

Florin, M.-V. and M. T. Bürkler (2017). Introduction to the IRGC Risk Governance Framework, *revised version*. Lausanne, Switzerland, EPFL International Risk Governance Center.

Folke, C. (2016). "Resilience (republished)." Ecology and Society **21**(4).

Folke, C., *et al.* (2016). "Social-ecological resilience and biosphere-based sustainability science." Ecology and Society **21**(3).

Foster, L. A., *et al.* (2015). How does complex adaptive system theory inform innovation in complex project-based organisations? ISPIM Innovation Symposium, The International Society for Professional Innovation Management (ISPIM).

Fowler, J. F. (2014). Survey Research Methods. Thousand Oaks, California, Sage.

Fraenkel, J. R., *et al.* (2012). How to design and evaluate research in education. New York, McGraw-Hill

Francis, R. and B. Bekera (2014). "A metric and frameworks for resilience analysis of engineered and infrastructure systems." Reliability Engineering & System Safety **121**: 90-103.

Fraser, J. R. S., *et al.* (2010). Enterprise Risk Management: Today's Leading Research and Best Practices for Tomorrow's Executives. Hoboken, NJ, Wiley.

Fraser, J. R. S. and B. J. Simkins (2016). "The challenges of and solutions for implementing enterprise risk management." Business Horizons **59**(6): 689-698.

Freeman, D. (2017). "Risk taking with background risk under recursive rank-dependent utility." Mathematical Social Sciences **87**: 72-74.

Friday, D., et al. (2018). "Collaborative risk management: a systematic literature review." International Journal of Physical Distribution & Logistics Management **48**(3): 231-253.

Fu, G., *et al.* (2016). "Anatomy of Tianjin Port fire and explosion: Process and causes." Process Safety Progress **35**(3): 216-220.

Gajjar, H., *et al.* (2013). Modelling the Economics of Port Resiliency. Ports 2013: Success through Diversification - Proceedings of Ports '13: 13th Triennial International Conference. B. I. Ostbo and D. Oates. Seattle, Washington US, American Society of Civil Engineers**:** 1706-1715.

Gaile, G. L. and C. J. Willmott (2005). Geography in America at the Dawn of the 21st Century, Oxford University Press on Demand.

Gallaire, H. (1998). Faster, connected, smarter! 21st century technologies: Promises and perils of a dynamic future. OECD. Paris, France, OECD Publishing**:** 47.

Gallina, V., *et al.* (2016). "A review of multi-risk methodologies for natural hazards: Consequences and challenges for a climate change impact assessment." Journal of environmental management **168**: 123-132.

Gallopín, G. C. (2006). "Linkages between vulnerability, resilience, and adaptive capacity." Global environmental change **16**(3): 293-303.

GAO (2007). Port Risk Management: Additional Federal Guidance Would Aid Ports in Disaster Planning and Recovery, Available online at https://www.gao.gov/products/GAO-07-412. Washington, DC, US Government Accountability Office.

Garber, D. (2005). Descartes, Rene (1596–1650). The Shorter Routledge Encyclopaedia of Philosophy. E. Craig. Abingdon, UK, Routledge.

Garcia-Aristizabal, A., *et al.* (2015). "Analysis of non-stationary climate-related extreme events considering climate change scenarios: an application for multi-hazard assessment in the Dar es Salaam region, Tanzania." Natural Hazards **75**(1): 289-320.

Garg, G. and C. R. Kothari (2014). Research methodology: Methods and techniques. New Delhi, India, New Age International Publishers.

Gatzert, N. and M. Martin (2015). "Determinants and value of enterprise risk management: empirical evidence from the literature." Risk Management and Insurance Review **18**(1): 29-53.

Gaudenzi, B. and A. Borghesi (2006). "Managing risks in the supply chain using the AHP method." The International Journal of Logistics Management **17**(1): 114-136.

Geerlings, H., *et al.*, Eds. (2018). Ports and Networks: Strategies, Operations and Perspectives. Abingdon, UK, Routledge.

Gharehgozli, A. H., *et al.* (2017). "Evaluating a “wicked problem”: A conceptual framework on seaport resiliency in the event of weather disruptions." Technological Forecasting and Social Change **121**: 65-75.

Giannakis, M. and T. Papadopoulos (2016). "Supply chain sustainability: A risk management approach." International Journal of Production Economics **171**: 455-470.

Gibson, C. A. and M. Tarrant (2010). "A 'conceptual models' approach to organisational resilience." Australian Journal of Emergency Management, The **25**(2): 6.

Gimenez, R., *et al.* (2017). "A maturity model for the involvement of stakeholders in the city resilience building process." Technological Forecasting and Social Change **121**: 7-16.

Girvin, S. (2017). The Safe Port in Maritime Law: Decade of Certainty or Muddier Waters? Available online at http://law.nus.edu.sg/cml/pdfs/wps/CML-WPS-1702.pdf. NUS Centre for Maritime Law Working Paper Singapore, National University of Singapore.

Glaser, B. G. and A. L. Strauss (1967). The discovery of grounded theory: Strategies for qualitative research. New Brunswick, US, Transaction publishers.

Glasow, P. A. (2005). Fundamentals of survey research methodology, available online at http://www.mitre.org/work/tech_papers/tech_papers_05/05_0638/05_0638.pdf. McLean, Virginia US, Mitre Corporation, department W804. **18**.

Glendon, A. I., *et al.* (2016). Human Safety and Risk Management. Boca Raton, FL, CRC Press.

Gliem, J. A. and R. R. Gliem (2003). Calculating, interpreting, and reporting Cronbach's alpha reliability coefficient for Likert-type scales, Midwest Research-to-Practice Conference in Adult, Continuing, and Community Education.

Golafshani, N. (2003). "Understanding reliability and validity in qualitative research." The Qualitative Report **8**(4): 597-606.

Goodwin, C. J. (2010). Research in psychology: Methods and design. Hoboken, NJ US, John Wiley & Sons.

Gopalakrishnan, K. and S. Peeta, Eds. (2010). Sustainable and Resilient Critical Infrastructure Systems: Simulation, Modelling, and Intelligent Engineering. Berlin, Germany, Springer Science & Business Media.

Gourley, T. (2007). Ship Underkeel Clearance in Waves. 18th Australasian Coastal and Ocean Engineering Conference 2007 and the 11th Australasian Port and Harbour Conference 2007 (Coasts and Ports 2007), 18-20 July Melbourne, VIC, Engineers Australia.

Government, Q. (2017). A Guide to Risk Management, Available online at https://www.treasury.qld.gov.au/resource/guide-risk-management/. Queensland Treasury. Brisbane, QLD, Queensland Government.

Graham, J. D. and J. B. Wiener, Eds. (1995). Risk vs. Risk: Tradeoffs in protecting health and the environment. Cambridge, MA, Harvard University Press.

Graham, J. D., *et al.* (2010). The Emergence of Risks: Contributing Factors. Geneva, Switzerland, International Risk Governance Council (IRGC).

Graham, J. D. and D. Kaye (2015). A Risk Management Approach to Business Continuity: Aligning Business Continuity and Corporate Governance. Brookfield, Connecticut USA, Rothstein Publishing.

Grant, R. M. (2016). Contemporary Strategy Analysis: Text and Cases Edition. Chichester, UK, Wiley.

Grant, A., *et al.* (2009). "GPS jamming and the impact on maritime navigation." The Journal of Navigation **62**(2): 173-187.

Gray, A. (2017). Port Risk and Resilience Management Survey. V. Justice**:** 1.

Grech, M. R., *et al.* (2008). Human Factors in the Maritime Domain. Boca Raton, Florida, CRC Press.

Grech, A., *et al.* (2013). "Guiding principles for the improved governance of port and shipping impacts in the Great Barrier Reef." Marine pollution bulletin **75**(1-2): 8-20.

Green, W. G. (2008a). Hazard analysis: The process of defining a hazard, Available online at www.pitt.edu/~super7/32011-33001/32791.ppt. Emergency Management Process Series No. 1. Pittsburgh, PA, University of Pittsburgh.

Green, W. G. (2008b). Hazard, Threats, Risk, Etc.: An examination of some key terms, Available online at www.pitt.edu/~super7/32011-33001/32341.ppt Disaster Theory Series No. 3. Pittsburgh, PA, University of Pittsburgh.

Greene, R. R. and A. P. Conrad (2002). Resilience: Basic assumptions and terms. Washington, DC, NASW Press.

Grinin, L., *et al.* (2016). Kondratieff waves in the world system perspective. Economic cycles, crises, and the global periphery. Cham, Switzerland, Springer**:** 23-54.

Guelke, C. (2005). A Strategic Approach to Disaster Preparedness. Engineering Management Conference (2005 IEEE International) St Johns, Canada, IEEE.

Guha-Sapir, D., *et al.* (2014). Annual Disaster Statistical Review: Numbers and Trends 2013. Brussels, Belgium, Centre for Research on the Epidemiology of Disasters

Guild, E. (2009). Security and Migration in the 21st Century. Cambridge, UK, Polity.

Gunasekaran, A. and B. Kobu (2007). "Performance measures and metrics in logistics and supply chain management: a review of recent literature (1995–2004) for research and applications." International Journal of Production Research **45**(12): 2819-2840.

Gunderson, L. H. (2000). "Ecological resilience—in theory and application." Annual Review of Ecology and Systematics **31**(1): 425-439.

Gurning, S. and S. Cahoon (2009). Analysis of random disruptive events in shipping and port operations. International Forum on Shipping, Ports and Airports (IFSPA 2009), Hongkong

Gurning, S. and S. Cahoon (2011). "Analysis of Multi-Mitigation Scenarios on Maritime Disruptions." Maritime Policy & Management: The flagship journal of international shipping and port research **38**(3): 251-268.

Haddow, G., *et al.*, Eds. (2017). Introduction to Emergency Management. Amsterdam, The Netherlands, Butterworth-Heinemann.

Haimes, Y. Y. (2008). "Models for Risk Management of Systems of Systems." International Journal of Systems Engineering **1**(1/2): 222-236.

Haimes, Y. Y. (2016). Risk modelling, assessment, and management. Hoboken, NJ, John Wiley & Sons.

Haimes, Y. Y. (2018). "Risk Modelling of Interdependent Complex Systems of Systems: Theory and Practice." Risk analysis **38**(1): 84-98.

Hall, R. (1992). "The strategic analysis of intangible resources." Strategic management journal **13**(2): 135-144.

Hall, R. (1993). "A framework linking intangible resources and capabilities to sustainable competitive advantage." Strategic management journal **14**(8): 607-618.

Hambridge, N. B., *et al.* (2017). "Coordination in Crises: Implementation of the National Incident Management System by Surface Transportation Agencies, Available online at https://www.hsaj.org/articles/13773." Homeland Security Affairs **13**: np.

Hamilton, D. C. (2011). Multilateral continuity planning. The Definitive Handbook of Business Continuity Management. A. Hiles. Chichester, UK, Wiley**:** 37-49.

Han, K., *et al.* (2017). "Relative Strategic Emphasis and Firm-Idiosyncratic Risk: The Moderating Role of Relative Performance and Demand Instability." Journal of Marketing **81**(4): 25-44.

Handfield, R. B. (2007) Reducing the Impact of Disruptions to the Supply Chain. Sascom.

Handley-Schachler, M. and J. Navare (2010). "Port Risk Management and Public Private Partnerships: Factors Relating to Risk Allocation and Risk Sustainability." World Review of Intermodal Transportation Research **3**(1/2): 150-166.

Hansson, S. O. and T. Aven (2014). "Is risk analysis scientific?" Risk analysis **34**(7): 1173-1183.

Haraguchi, M. and S. Kim (2014). Critical infrastructure systems: A case study of the interconnectedness of risks posed by Hurricane Sandy for New York city. Global Assessment Report on Disaster Risk Reduction 2015, United Nations Office for Disaster Risk Reduction.

Haraguchi, M., *et al.* (2016). "Building Private Sector Resilience: Directions After the 2015 Sendai Framework." Journal of Disaster Research **11**(3): 535-543.

Häring, I., *et al.* (2017). Towards a Generic Resilience Management, Quantification and Development Process: General Definitions, Requirements, Methods, Techniques and Measures, and Case Studies. Resilience and Risk. I. Linkov and J. M. Palma-Oliveira. Dordrecht, The Netherlands, Springer**:** 21-80.

Harland, L., *et al.* (2005). "Leadership behaviors and subordinate resilience." Journal of Leadership & Organizational Studies **11**(2): 2-14.

Harner, M. M. (2010). "Ignoring the writing on the wall: the role of Enterprise risk management in the economic crisis." Journal of Business & Technology Law **5**(1): 45.

Harrington, H. J. (2006). The Five Pillars of Organizational Excellence, Quality Digest. Chico, CA, QCI International.

Harrington, S. E., *et al.* (2011). Enterprise risk management: The case of United Grain growers. Structured Finance and Insurance: The ART of Managing Capital and Risk. C. L. Culp, John Wiley & sons**:** 744-763.

Harris-Hogan, S. (2017). "Violent extremism in Australia: An overview." Trends and Issues in Crime and Criminal Justice (491): 1.

Harrison III, R. L. (2013). "Using mixed methods designs in the Journal of Business Research, 1990–2010." Journal of Business Research **66**(11): 2153-2162.

Hartwich, O. M. (2012). Faraway, So Close: How the Euro Crisis Affects Australia. Issue Analysis 23 April. Sydney, Australia, The Centre for Independent Studies. **132**.

Hay, A. H. (2016). "The incident sequence as resilience planning framework." Infrastructure Asset Management **3**(2): 55-60.

Hayes, J. (2014). A new policy direction in Australian offshore safety regulation. Risk Governance of Offshore Oil and Gas Operations. P. H. Lindøe, M. Baram and O. Renn. New York, NY, Cambridge University Press**:** 188.

Hayes, P. and C. Owen (2017). Human Factors in Emergency Management. Human factors challenges in emergency management: Enhancing individual and team performance in fire and emergency services. C. Owen. London, UK, CRC Press**:** 17-34.

Hayne, C. and C. Free (2014). "Hybridized professional groups and institutional work: COSO and the rise of enterprise risk management." Accounting, organizations and society **39**(5): 309-330.

Heath-Kelly, C., *et al.* (2015). "Editors' introduction: Neoliberalism and/as terror." Critical Studies on Terrorism **8**(1): 1-14.

Head, B. W. and J. Alford (2015). "Wicked problems: Implications for public policy and management." Administration & Society **47**(6): 711-739.

Heaver, T. D. (2009). Co-ordination in Multi-Actor Logistics Operations: Challenges at the Port Interface. Workshop on Integrating Maritime Transport in Value Chains, June 10-12. Montreal, Canada.

Heffron, R., *et al.* (2016). PIANC Guidelines: Oil and Petrochemical Terminal Design. Ports 2016, 14th Triennial International Conference, June 12–15, New Orleans, Louisiana, American Society of Civil engineers.

Heilig, L. and S. Voß (2017a). A framework and categorisation. Ports and Networks: Strategies, Operations and Perspectives. H. Geerlings, B. Kuipers and R. Zuidwijk. Abingdon, UK, Routledge.

Heilig, L. and S. Voß (2017b). "Information systems in seaports: a categorization and overview." Information Technology and Management **18**(3): 179-201.

Helfat, C. E. and M. A. Peteraf (2015). "Managerial cognitive capabilities and the microfoundations of dynamic capabilities." Strategic management journal **36**(6): 831-850.

Hellingrath, B., *et al.* (2015). Disaster Management Capacity Building at Airports and Seaports. Humanitarian Logistics and Sustainability. M. Klumpp, S. de Leeuw, A. Regattieri and R. de Souza. Cham, Switzerland, Springer International Publishing**:** 87-112.

Henderson, R. M., *et al.* (2017). Climate change in 2017: Implications for business, Boston, MA, Harvard Business School.

Herrick, C. and J. Pratt (2012). "Sustainability in the Water Sector: Enabling lasting change through leadership and cultural transformation." Nature and Culture **7**(3): 285-313.

Hewson, C. and D. W. Stewart (2016). Internet research methods. Communication and technology. J. A. Danowski and L. Cantoni. Berlin, Germany, De Gruyter Mouton.

Hiles, A., Ed. (2011). The definitive handbook of business continuity management. Chichester, UK, John Wiley & Sons.

Hill, C. W. L., *et al.* (2014). Strategic management: theory: an integrated approach. Stamford, CT, Cengage Learning.

Hillson, D. (2005). Effective opportunity management for projects: Exploiting positive risk. New York, NY, Marcel Dekker.

Hillson, D. and R. Murray-Webster (2017). Understanding and managing risk attitude. Abingdon, UK, Routledge.

Hinkel, J. (2011). "Indicators of vulnerability and adaptive capacity: towards a clarification of the science–policy interface." Global environmental change **21**(1): 198-208.

Hinton, P. R., *et al.* (2014). SPSS explained. London, Routledge.

Ho, W., *et al.* (2015). "Supply chain risk management: a literature review." International Journal of Production Research **53**(16): 5031-5069.

Hodkinson, P. and H. Hodkinson (2001). The strengths and limitations of case study research. Making an Impact on Policy and Practice, 5-7 December. Cambridge, UK. **1:** 5-7.

Hodgkinson, J. H., *et al*. (2014). "Climate adaptation in Australia's resource-extraction industries: ready or not?" Regional environmental change **14**(4): 1663-1678.

Hoinville, G. and R. Jowell, Eds. (1985). Survey Research Practice. Aldershot, UK, Gower.

Holling, C. S. (1973). "Resilience and Stability of Ecological Systems." Annual Review of Ecology and Systematics **4**: 1-23.

Holling, C. S. (2001). "Understanding the complexity of economic, ecological, and social systems." Ecosystems **4**(5): 390-405.

Holling, C. S. and L. H. Gunderson (2002). Resilience and Adaptive Cycles. Panarchy: Understanding Transformations in Human and Natural Systems. L. H. Gunderson and C. S. Holling. Washington, US, Island Press.

Hollnagel, E. (2009) The Resilient Organisation.

Hollnagel, E. (2014). "Resilience engineering and the built environment." Building Research & Information **42**(2): 221-228.

Hollnagel, E. (2017). FRAM: the functional resonance analysis method: Modelling complex socio-technical systems. Farnham, UK, CRC Press.

Hollnagel, E. and Y. Fujita (2013). "The Fukushima disaster–systemic failures as the lack of resilience." Nuclear Engineering and Technology **45**(1): 13-20.

Hollnagel, E., *et al.*, Eds. (2012). Resilience Engineering: Concepts and Precepts Aldershot, UK, Ashgate Publishing, Ltd.

Hong, Y. (2017). "Motivation behind China's 'One Belt, One Road' Initiatives and Establishment of the Asian Infrastructure Investment Bank." Journal of Contemporary China **26**(105): 353-368.

Hooper, N., *et al.* (2018). Failing the sunlight test, Available online at https://companydirectors.partica.online/aicd-company-directors/cd-june-2018/flipbook/8/. Australian Institute of Company Directors. Sydney, NSW, AICD**:** 16-26.

Hopkin, P. (2017). Fundamentals of risk management: understanding, evaluating and implementing effective risk management, Kogan Page Publishers.

Hosseini, S., *et al.* (2016). "A review of definitions and measures of system resilience." Reliability Engineering & System Safety **145**: 47-61.

Houghton, R. J., *et al.* (2006). "Command and control in emergency services operations: a social network analysis." Ergonomics **49**(12-13): 1204-1225.

Hox, J. J., *et al.* (2017). Multilevel analysis: Techniques and applications. New York, NY, Routledge.

Hoyle, B. (2000). "Global and local change on the port-city waterfront." Geographical Review **90**(3): 395-417.

Hoyt, R. E. and A. P. Liebenberg (2011). "The value of enterprise risk management." Journal of risk and insurance **78**(4): 795-822.

Hrnjic, E., *et al.* (2015). Styles of Financial Management. Unpublished manuscript. New York, NY, The Center for Global Enterprise.

Hsieh, C.-H., *et al.* (2014). "Port vulnerability assessment from the perspective of critical infrastructure interdependency." Maritime Policy and Management **41**(6): 589-606.

Hsu, W-K. K. (2015). "Assessing the Safety Factors of Ship Berthing Operations." Journal of Navigation **68**(3): 576-588.

Hubbard, D. W. (2009). The failure of risk management: Why it's broken and how to fix it. Hoboken, NJ, John Wiley & Sons.

Hughes, J. F. and K. Healy (2014). Measuring the resilience of transport infrastructure. NZ Transport Agency research report 546. Wellington, NZ, New Zealand Transport Agency.

Hunt, P. and I. Greaves (2017). Oxford Manual of Major Incident Management. Oxford, UK, Oxford University Press.

IA (2016). Australian Infrastructure Plan: Priorities and reforms for our nation's future, Available online at http://infrastructureaustralia.gov.au/policy-publications/publications/Australian-Infrastructure-Plan.aspx. Policy and Publications. Sydney, NSW, Infrastructure Australia.

IALA (2016). Vessel Traffic Services Manual. Saint Germain en Laye, France, International Association of Marine Aids to Navigation and Lighthouse Authorities (IALA).

Inan, D. I., *et al.* (2016). Towards knowledge sharing in disaster management: An agent-oriented knowledge analysis framework. Australasian Conference on Information Systems. Adelaide, SA.

Inglis, J., *et al.* (2014). Climate adaptation manual for local government: Embedding resilience to climate change. Sydney, NSW, University of Technology.

IRGC (2011). Improving the management of emerging risks. Concept Notes. Geneva, Switzerland, International Risk Governance Council.

IRGC (2015). IRGC guidelines for emerging risk governance: Guidance for the governance of unfamiliar risks. Concept Notes. O. Renn. Geneva, Switzerland, International Risk Governance Council.

ISO (2002). 73:2002. Guide 73, Risk Management-Vocabulary-Guidelines for Use in Standards. Geneva, Switzerland, International Standards Organisation.

ISO (2009). 73:2009: Risk management vocabulary. Geneva, Switzerland, International Organization for Standardization.

ISO (2011). ISO/IEC 27031:2011 Information technology -- Security techniques -- Guidelines for information and communication technology readiness for business continuity. Geneva, Switzerland, International Organization for Standardization.

ISO (2012). ISO/IEC 27032:2012 Information technology -- Security techniques -- Guidelines for cybersecurity. Geneva, Switzerland, International Organization for Standardization.

ISO (2018). ISO 31000:2018: Risk Management - Principles and Guidelines Geneva, Switzerland, International Organisation for Standardisation.

ISO (2012). ISO 22301:2012 Business Continuity Management Geneva, Switzerland, International Organization for Standardization.

ISO (2017). ISO 22316:2017 - Security and resilience — Organizational resilience — Principles and attributes. Geneva, Switzerland, International Organization for Standardization.

ISO (2018). Standards Catalogue, Available online at https://www.iso.org/standards-catalogue/browse-by-ics.html. Geneva, Switzerland, International Organization for Standardization.

Ivanov, D., *et al.* (2014). "The Ripple effect in supply chains: Trade-off efficiency-flexibility-resilience in disruption management." International Journal of Production Research **52**(7): 2154-2172.

Jansen, K. J., *et al.* (2007). E-survey methodology. Handbook of research on electronic surveys and measurements. R. A. Reynolds, R. Woods and J. D. Baker. Hershey, PA US, Idea Group**:** 1-8.

Janssen, M. A., *et al.* (2007). "Robustness of social-ecological systems to spatial and temporal variability." Society and Natural Resources **20**(4): 307-322.

Jenkins, S. (2015). "Resilience: The new paradigm in disaster management—An Australian perspective." World Journal of Engineering and Technology **3**(03): 129.

Jia, G., *et al.* (2013). "Measuring the maturity of risk management in large-scale construction projects." Automation in Construction **34**: 56-66.

Johansen, W., *et al.* (2011). Entering New Territory: The Study of Internal Crisis Management and Crisis Communication in Organizations. 18th BledCom public relations conference. Lake Bled, Slovenia.

Johansson, J. and H. Hassel (2010). "An approach for modelling interdependent infrastructures in the context of vulnerability analysis." Reliability Engineering & System Safety **95**(12): 1335-1344.

John, A. and T. C. Nwaoha (2016). "Safety critical maritime infrastructure systems resilience: A critical review." International Journal of Maritime Engineering **158**: A209-A217.

John, A., *et al.* (2015). "A new approach for evaluating the disruption risks of a seaport system." Safety and reliability: methodology and applications. London: Taylor & Francis Group: 591-598.

John, A., *et al.* (2016). "A risk assessment approach to improve the resilience of a seaport system using Bayesian networks." Ocean Engineering **111**: 136-147.

John, A., *et al.* (2018). A Decision Support System for the Assessment of Seaports' Security Under Fuzzy Environment. Modelling, Computing and Data Handling Methodologies for Maritime Transportation. C. Konstantopoulos and G. Pantziou. Cham, Switzerland, Springer**:** 145-177.

Johnson, R. B. and A. J. Onwuegbuzie (2004). "Mixed methods research: A research paradigm whose time has come." Educational researcher **33**(7): 14-26.

Jones, B. A. (2015). Benchmarking organizational resilience: A cross-sectional comparative research study. New Jersey, US, New Jersey City University.

Jonkeren, O. and P. Rietveld (2016). "Protection of Critical Waterborne Transport Infrastructures: An Economic Review." Transport Reviews **36**(4): 437-453.

Joyce, K. E., *et al*. (2014). "Mapping and monitoring geological hazards using optical, LiDAR, and synthetic aperture RADAR image data." Natural hazards **73**(2): 137-163.

Judek, C. and A.-M. Edjossan-Sossou (2017). Crisis and emergency situation: Simulation considering cascading effects methodology. Lorraine, France, University of Lorraine.

Jupp, V. (2006). The Sage Dictionary of Social Research Methods. London, UK, Sage Publications.

Justice, V. (2016). Minimising Shipping Delays: Managing Black Swan events in Australian ports. World Maritime Day 2016, 13 October. Australian Maritime College – Launceston, Tasmania.

Jüttner, U., *et al.* (2003). "Supply Chain Risk Management: Outlining an Agenda for Future Research." International Journal of Logistics: Research & Applications **6**(4): 197-210.

Kaim, A., *et al.* (2012). Organisational change - A detailed study on organisational change. Delhi, India, University of Delhi.

Kaplan, R. S. and A. Mikes (2012). "Managing Risks: A New Framework." Harvard Business Review **90**(6): 48-60.

Kappes, M. S., *et al.* (2012). "Challenges of analyzing multi-hazard risk: a review." Natural Hazards **64**(2): 1925-1958.

Karlsson, F., *et al.* (2017). "Inter-organisational information sharing in the public sector: A longitudinal case study on the reshaping of success factors." Government Information Quarterly **34**(4): 567-577.

Kasperson, R. E., *et al.* (1988). "The social amplification of risk: A conceptual framework." Risk analysis **8**(2): 177-187.

Kavina, C. (2017). "Safe and sound in the eye of the storm." 2017, from https://www.flindersports.com.au/projects/sa/.

Kay, B. (2011) South Korean Tech Companies Pick up Slack Left by Japan. The Christian Science Monitor.

Kayes, D. C. (2015). Organizational resilience: How learning sustains organizations in crisis, disaster, and breakdown. New York, NY, Oxford University Press.

Keim, M. E. (2015). The public health impacts of natural disasters. Handbook of public health in natural disasters R. R. Watson, J. A. Tabor, J. E. Ehiri and V. R. Preedy. Wageningen, Netherlands, Wageningen Academic Publishers. **10:** 33.

Kelly-Hope, L. A., *et al.* (2004). "Ross River virus disease in Australia, 1886–1998, with analysis of risk factors associated with outbreaks." Journal of Medical Entomology **41**(2): 133-150.

Kelman, I., *et al.* (2017). The Routledge handbook of disaster risk reduction including climate change adaptation. Abingdon, UK, Routledge.

Khazai, B., *et al.* (2015). A guide to measuring urban risk resilience: Principles, tools and practice of urban indicators. Earthquakes and Megacities Quezon City, The Philippines, Earthquakes and Megacities Initiative.

Kiem, A. S., *et al.* (2016). "Natural hazards in Australia: Droughts." Climatic Change **139**(1): 37-54.

Kilgariff, M. (2017). Australian Government's role in the development of cities. Submission to Standing Committee on Infrastructure, Transport and Cities. Canberra, ACT, Australian Logistics Council.

Kim, S. D. (2012). Characterizing unknown unknowns. PMI® Global Congress 2012—North America. Vancouver, British Columbia, Canada, Project Management Institute.

Kim, E. and H. Park (2018). "Two-stage approach to quantify the resilience of maritime hazardous and noxious substance spill accidents." International Journal of Disaster Risk Reduction **28**: 595-601.

Kirsch, L. S. (1997). "Portfolios of control modes and IS project management." Information systems research **8**(3): 215-239.

Kisfalvi, V. and S. Maguire (2011). "On the nature of institutional entrepreneurs: Insights from the life of Rachel Carson." Journal of Management Inquiry **20**(2): 152-177.

Kleindorfer, P. R. and G. H. Saad (2005). "Managing Disruption Risks in Supply Chains." Production and Operations Management **14**(1): 53-68.

Kline, R. B. (2016). Principles and practice of structural equation modelling. New York, NY, Guilford Publications.

Knight, K. W. (2006). Risk management a journey not a destination. Executive Meeting, 20 May. Angra Dos Reis, Brazil.

Knight, K. W. (2009). Transitioning to the new risk management standard AS/NZS/ISO 31000:2018. Comcover Insurance and Risk Management Conference, 27 August. Canberra, ACT, Australian Government - Department of Finance and Deregulation.

Kobayashi, K. (2013). "Unforeseen risk and planning perspectives." Journal of Japan Society of Civil engineers **69**(5): 431-446.

Kok, M., *et al.* (2016). "A new method for analysing socio-ecological patterns of vulnerability." Regional environmental change **16**(1): 229-243.

Kolář, P. and S. M. Puckett (2011). Role of port authorities in Australia, Canada and the European Union, Available online at http://www.patrec.org/atrf.aspx. Australasian Transport Research Forum 2011 Proceedings, 28 - 30 September Adelaide, SA.

Kolomiyets, T. (2017). Risk management maturity model, Available online at https://statswiki.unece.org/display/GORM/7.+Risk+management+information+system. Guidelines on risk management practices in statistical organizations Geneva, Switzerland, United Nations Economic Commission for Europe (UNECE).

Konings, J. W. (2008). The future of intermodal freight transport: operations, design and policy. Cheltenham, UK, Edward Elgar Publishing.

Koschatzky, V. and F. E. D. de Oliveira (2016). "Earthquake scenario." National Emergency Response **29**(4): 12.

Kouns, J. and D. Minoli (2010). Information Security Risk Management. Hoboken, NJ, John Wiley & Sons.

Kristiansen, S. (2013). Maritime Transportation: Safety Management and Risk Analysis. Abingdon, UK, Routledge.

Krosnick, J. A. (2018). Questionnaire design. The Palgrave Handbook of Survey Research. V. D. and K. J. Cham, Switzerland, Palgrave Macmillan**:** 439-455.

Kunreuther, H. and M. V. Pauly (2010). Insuring against Catastrophes. The Known, the Unknown, and the Unknowable in Financial Risk Management: Measurement and Theory Advancing Practice. F. X. Diebold, N. A. Doherty and R. J. Herring. Princeton, NJ, Princeton University press**:** 210.

Kuo, S.-Y., *et al.* (2017). "The effects of dynamic capabilities, service capabilities, competitive advantage, and organizational performance in container shipping." Transportation research part A: policy and practice **95**: 356-371.

Kurtz, D. J. and G. Varvakis (2016). Dynamic capabilities and organizational resilience in turbulent environments. Competitive strategies for small and medium enterprises. North and G. Varvakis. Cham, Switzerland, Springer**:** 19-37.

Kwok, A. H., *et al.* (2016). "What is 'social resilience'? Perspectives of disaster researchers, emergency management practitioners, and policymakers in New Zealand." International Journal of Disaster Risk Reduction **19**: 197-211.

Kyoto University (2009). International Workshop on Risk Governance of the Maritime Global Critical Infrastructure: Straits of Malacca and Singapore Exposed to Extreme Hazards, June 4 and 5, 2009. Maritime GCI Summary Workshop Report. Geneva, International Risk Governance Council.

Labaka, L., *et al.* (2016). "A holistic framework for building critical infrastructure resilience." Technological Forecasting and Social Change **103**: 21-33.

Labaka-Zubieta, L. (2013). Resilience Framework for Critical Infrastructures. European Journal of Operational Research. San Sebastian, University of Navarra. PhD Thesis.

Lam, D. R. (2017). Extreme flood events in South East Queensland: evidence and implications. School of Earth and Environmental Sciences. Brisbane, QLD, The University of Queensland.

Lam, J. (2014). Enterprise risk management: from incentives to controls. Hoboken, NJ, John Wiley & Sons.

Lam, J. S. L. and K.-H. Lai (2015). "Developing environmental sustainability by ANP-QFD approach: the case of shipping operations." Journal of Cleaner Production **105**: 275-284.

Lam, J. S. L. and S. Su (2015). "Disruption risks and mitigation strategies: an analysis of Asian ports." Maritime Policy & Management **42**(5): 415-435.

Lam, J. S. L. and T. L. Yip (2012). Impact of port disruption on supply chains: A Petri net approach. Third International Conference on Computational Logistics, Shanghai, China, September 24-26, Springer.

Lam, J. S.-L. and J. A. Lassa (2017). "Risk assessment framework for exposure of cargo and ports to natural hazards and climate extremes." Maritime Policy & Management **44**(1): 1-15.

Langer, M. (2017). "Developing a Data Backup Strategy." Risk Management **64**(10): 12-13.

Lansdale, A. (2012). The Work of the Harbourmaster: A Practical Guide. London, UK, Nautical Institute (Great Britain).

Lantsman, L. (2017). Seaport Vulnerability to Criminal Networks: A Mixed Method Approach to Measuring Criminological Vulnerability in the Top 30 US Container Ports. New York, NY, City University of New York.

Lark, J. (2015). ISO31000: Risk Management: A Practical Guide for SMEs. Geneva, Switzerland, International Organization for Standardization

Lavrakas, P. J. (2008). Encyclopaedia of survey research methods. Thousand Oaks, CA, SAGE Publications.

Lawrence, V., *et al.* (2017). CFD simulation of passenger hazard risk at railway station platforms due to explosive air blasts. The 4th Thailand Rail Academic Symposium (TRAS 2017) August 31 – September 1. Khao Yai, Pakchong, Nakhon Ratchasima, Thailand, Massachusetts Institute of Technology.

Lebel, L., *et al.* (2006). "Governance and the capacity to manage resilience in regional social-ecological systems." Ecology and Society **11**(1).

Lee, A. V., *et al.* (2013). "Developing a tool to measure and compare organizations' resilience." Natural Hazards Review **14**(1): 29-41.

Lengnick-Hall, C. A., *et al.* (2011). "Developing a capacity for organizational resilience through strategic human resource management." Human Resource Management Review **21**(3): 243-255.

Leonard-Barton, D. (1998). Wellspring of knowledge. Boston, MA, Harvard Business School Press.

Leveson, N. (2015). "A systems approach to risk management through leading safety indicators." Reliability Engineering & System Safety **136**: 17-34.

Leveson, N. G. (2017). Engineering a safer world. Cambridge, MA, MIT Press.

Levin, K., *et al*. (2012). "Overcoming the tragedy of super wicked problems: constraining our future selves to ameliorate global climate change." Policy Sciences **45**(2): 123-152.

Levine, S. (2014). Assessing resilience: Why quantification misses the point. Humanitarian Policy Group (ODI) Working Paper. London, UK, Overseas Development Institute.

Lewis, L. (2017). Port communications policies. V. Justice. Brisbane, QLD**:** 1.

Li, H., *et al.* (2017). "Enhancement of supply chain resilience through inter-echelon information sharing." Flexible Services and Manufacturing Journal **29**(2): 260-285.

Liebenberg, A. P. and R. E. Hoyt (2003). "The determinants of enterprise risk management: Evidence from the appointment of chief risk officers." Risk Management and Insurance Review **6**(1): 37-52.

Liu, Z., et al. (2015). "A three-level framework for multi-risk assessment." Georisk: Assessment and Management of Risk for Engineered Systems and Geohazards **9**(2): 59-74.

Likert, R. (1932). "A technique for the measurement of attitudes." Archives of psychology.

Likert, R., *et al.* (1934). "A simple and reliable method of scoring the Thurstone attitude scales." The Journal of Social Psychology **5**(2): 228-238.

Lincoln, Y. S. and E. G. Guba (1985). Naturalistic inquiry. Newberry Park, CA, Sage.

Lindbom, H., *et al.* (2015). "The capability concept–On how to define and describe capability in relation to risk, vulnerability and resilience." Reliability Engineering & System Safety **135**: 45-54.

Linkov, I., *et al.* (2014). "Changing the resilience paradigm." Nature Climate Change **4**(6): 407.

Linnenluecke, M. K. (2017). "Resilience in business and management research: A review of influential publications and a research agenda." International Journal of Management Reviews **19**(1): 4-30.

Linnenluecke, M. K. and A. Griffiths (2013). "Firms and sustainability: Mapping the intellectual origins and structure of the corporate sustainability field." Global environmental change **23**(1): 382-391.

Liu, H., *et al.* (2018). "Analysis of vulnerabilities in maritime supply chains." Reliability Engineering & System Safety **169**: 475-484.

Liu, W. (2014). "The application of resilience assessment-resilience of what, to what, with what? A case study based on Caledon, Ontario, Canada." Ecology and Society **19**(4): 1-25.

Loh, H. S. and V. V. Thai (2014). "Managing Port-Related Supply Chain Disruptions: A Conceptual Paper." The Asian Journal of Shipping and Logistics **30**(1): 97-116.

Loh, H. S. and V. V. Thai (2015). "Management of disruptions by seaports: preliminary findings." Asia Pacific Journal of Marketing and Logistics **27**(1): 146-162.

Losada, C., *et al.* (2012). "Optimizing system resilience: A facility protection model with recovery time." European Journal of Operational Research **217**: 519-530.

Lovrić, M., *et al.* (2017). "A conceptual design for a national transport model with cross-sectoral interdependencies." Transportation Research Procedia **27**: 720-727.

Lowinger, S., *et al.* (2016). "Interdependent lattice networks in high dimensions." Physical Review E **94**(5): 052306.

Lowrance, W. W. (1976). Of Acceptable Risk. Los Altos, California US, William Kauffman.

Lozano, R. (2015). "A holistic perspective on corporate sustainability drivers." Corporate Social Responsibility and Environmental Management **22**(1): 32-44.

Lyles, M. A. (2014). "Organizational Learning, knowledge creation, problem formulation and innovation in messy problems." European Management Journal **32**(1): 132-136.

MacKenzie, C. A. (2012). Interdependent Impacts of Disruption Management: Risk-Based Applications to Port Closures, Natural Disasters, and Oil Spills. School of Industrial Engineering. Oklahoma, US, The University of Oklahoma. PhD Thesis.

Madani, S. (2018). Global seaport competitiveness: a resource management perspective. School of Business IT and Logistics. Melbourne, Vic, RMIT University.

Mandaraka-Sheppard, A. (2014). Modern Maritime Law and Risk Management. London, UK, Informa Law.

Manfield, R. C. (2016). Organizational resilience: A dynamic capabilities approach. University of Queensland Business School. Brisbane, QLD, University of Queensland. PhD Thesis.

Manuele, F. A. (2013). On the Practice of Safety. Hoboken, US, John Wiley & Son.

Manuti, A., *et al.* (2015). "Formal and informal learning in the workplace: a research review." International journal of training and development **19**(1): 1-17.

Marcus, B., *et al.* (2017). "The use of snowball sampling for multi-source organizational research: Some cause for concern." Personnel Psychology **70**(3): 635-673.

Marsh (2014). Ports and terminals: Risk challenges and solutions Global Infrastructure and Marine Practices. London, UK, Marsh & McLennan Companies' Global Infrastructure Services.

Marshall, B., *et al.* (2013). "Does sample size matter in qualitative research? A review of qualitative interviews in is research." Journal of Computer Information Systems **Fall, 2013**: 11-22.

Marshall, C. and G. B. Rossman (2014). Designing qualitative research. Singapore, Sage publications.

Marshall, R. (2016). "Break free blocks Newcastle harbour." Green Left Weekly (1095): 3.

Mason-Jones, R. and D. R. Towill (1998). "Shrinking the Supply Chain Uncertainty Circle." Control September: 17-22.

Mattsson, L.-G. and E. Jenelius (2015). "Vulnerability and resilience of transport systems–a discussion of recent research." Transportation research part A: policy and practice **81**: 16-34.

Mauelshagen, C. W. (2012). Opening the black box: What makes risk management pervasive in organisations? School of Applied Sciences. Cranfield, UK, Cranfield. PhD Thesis.

Maunsell (2008). Impact of Climate Change on Infrastructure on Australia and CGE model inputs, Garnaut Climate Change Review. Melbourne, VIC, Cambridge University Press.

Mayhorn, C. B. and A. C. McLaughlin (2014). "Warning the world of extreme events: A global perspective on risk communication for natural and technological disaster." Safety science **61**: 43-50.

Mayoh, J. and A. J. Onwuegbuzie (2015). "Toward a conceptualization of mixed methods phenomenological research." Journal of mixed methods research **9**(1): 91-107.

Mazaheri, A., *et al.* (2015). "Usability of accident and incident reports for evidence-based risk modelling–A case study on ship grounding reports." Safety Science **76**: 202-214.

McBride, J. (2012). The estimated cost of tropical cyclone impacts in Western Australia. Technical Report for the Indian Ocean Climate Initiative (IOCI) Stage 3. Project 2.2: Tropical Cyclones in the North West. Melbourne, VIC, Bureau of Meteorology: Centre for Australian Weather and Climate research.

McCrae (2015). Close Calls: Managing Risk and Resilience in Airline Flight Safety. Basingstoke, UK, Palgrave.

McDaniels, T., *et al*. (2008). "Fostering resilience to extreme events within infrastructure systems: Characterizing decision contexts for mitigation and adaptation." Global Environmental Change **18**(2): 310-318.

McDonald, J. H. (2014). "Small numbers in chi-square and G-tests." Handbook of biological statistics: 86-89.

McDonald, M., *et al.* (2018). "Risk-Based Policy Optimization for Critical Infrastructure Resilience against a Pandemic Influenza Outbreak." ASCE-ASME Journal of Risk and Uncertainty in Engineering Systems, Part A: Civil Engineering **4**(2): 04018007.

McEvoy, D. and J. Mullett (2013). Enhancing the resilience of Seaports to a Changing Climate: Research Synthesis and Implications for Policy and Practice. Gold Coast, Australia, National Climate Change Adaptation Research Facility (NCCARF).

McEvoy, D., *et al.* (2013). Understanding future risks to ports in Australia. Enhancing the resilience of seaports to a changing climate report series. Gold Coast, Queensland, National Climate Adaptation Research Facility. **21**.

McEvoy, D., *et al.* (2015). A decision support toolkit for climate resilient seaports in the Pacific region. Climate Change and Adaptation Planning for Ports. A. K. Y. Ng, A. Becker, S. Cahoon *et al.* Abingdon, UK, Routledge**:** 215.

McKinnon, A. (2006). "Life Without Trucks: The Impact of a Temporary Disruption of Road Freight Transport on a National Economy." Journal of Business Logistics **27**(2): 227-250.

McKinnon, A. (2009). "Administrative Shortcomings and their Legal Implications in the Context of Safe Ports." Australian and New Zealand Maritime Law Journal **23**: 186-204.

Mclaughlin, H. and C. Fearon (2013). "Understanding the development of port and regional relationships: a new cooperation/competition matrix." Maritime Policy & Management **40**(3): 278-294.

McManus, S., *et al.* (2007). Resilience management: a framework for assessing and improving the resilience of organisations. Canterbury, NZ, Resilient Organisations.

McManus, S., *et al.* (2008). "Facilitated process for improving organizational resilience." Natural Hazards Review **9**(2): 81-90.

McNab, D. (2015). Waterfront: Graft, corruption and violence - Australia's crime frontier from 1788 till now. Sydney, NSW, Hachette Australia.

McPeake, J., *et al.* (2014). "Electronic surveys: How to maximise success." Nurse Researcher **21**(3): 24.

Melnyk, S. A., *et al.* (2014). "Is performance measurement and management fit for the future?" Management Accounting Research **25**(2): 173-186.

Mentzer, J. T., *et al.* (2001). "Defining Supply Chain Management." Journal of Business Logistics **22**(2): 1-25.

Meterko, M., *et al.* (2015). "Response rates, nonresponse bias, and data quality: Results from a national survey of senior healthcare leaders." Public Opinion Quarterly **79**(1): 130-144.

Meuser, J. D., *et al.* (2016). "A network analysis of leadership theory: The infancy of integration." Journal of Management **42**(5): 1374-1403.

Meyer-Larsen, N. and R. Müller (2018). Enhancing the Cybersecurity of Port Community Systems. International Conference on Dynamics in Logistics, 20-22 February, Bremen, Germany, Springer.

Mikes, A. and A. Migdal (2014). Learning from the Kursk Submarine Rescue Failure: The Case for Pluralistic Risk Management, Harvard Business School.

Miklosik, A. (2015). "Improving project management performance through capability maturity measurement." Procedia Economics and Finance **30**: 522-530.

Miles, M. B. and A. M. Huberman (1994). Qualitative data analysis: An expanded sourcebook, sage.

Miles, M. B., *et al.* (2013). Qualitative Data Analysis: A Methods Sourcebook. Thousand Oaks, CA, SAGE Publications.

Miller, J. and N. Quinn (2017). Exercise Westwind – A collaborative oil spill response by oil & gas operators and agencies. International Oil Spill Conference Proceedings, May 15-18, Long Beach, CA, International Oil Spill Conference.

Mitchell, T. and K. Harris (2012). Resilience: A Risk Management Approach. Background Note. London, UK, Overseas Development Institute. January.

Modarres, M. (2016). Risk Analysis in Engineering: Techniques, Tools, and Trends. Boca Raton, FA, CRC Press.

Modica, M. and R. Zoboli (2016). "Vulnerability, resilience, hazard, risk, damage, and loss: a socio-ecological framework for natural disaster analysis." Web Ecology **16**(1): 59-62.

Mokhtari, K., *et al.* (2012). "Decision support framework for risk management on sea ports and terminals using fuzzy set theory and evidential reasoning approach." Expert Systems with Applications **39**(5): 5087-5103.

Montibeller, G. and D. Winterfeldt (2015). "Cognitive and motivational biases in decision and risk analysis." Risk analysis **35**(7): 1230-1251.

Morris, L., *et al.* (2016). Ports Resilience Index: A Port Management Self-Assessment. GOMSG-H-16-001. Seattle, Washington US, National Oceanic and Atmospheric Administration.

Morris, L. L. (2017). Ports Resilience Index: Participatory Methods to Assess Resilience. Baton Rouge, LA, Louisiana State University.

Mostashari, A., *et al.* (2011). "A Cognitive Process Architecture Framework for Secure and Resilient Seaport Operations." Marine Technology Society Journal **45**(3): 120-127.

Moteff, J. D. (2012). Critical infrastructure resilience: the evolution of policy and programs and issues for Congress, Available online at https://cyberwar.nl/d/R42683.pdf. CRS Report for Congress. Washington, DC, Congressional Research Service US.

Moynihan, D. P. (2008). "Learning under uncertainty: Networks in crisis management." Public Administration Review **68**(2): 350-365.

Mullett, J and M. D. (2011). Climate resilient seaports. Proceedings of the 20th Australasian Coastal and Ocean Engineering Conference and the 13th Australasian Port and Harbour Conference: Coasts and Ports, 2011: Diverse and Developing Cairns, QLD, Engineers Australia.

Mutton, J. (2012). "Do I really need a risk register?" Keeping good companies **64**(8): 469.

Nair, A., *et al.* (2014). "Enterprise risk management as a dynamic capability: A test of its effectiveness during a crisis." Managerial and Decision Economics **35**(8): 555-566.

Naish, S., *et al.* (2014). "Climate change and dengue: a critical and systematic review of quantitative modelling approaches." BMC infectious diseases **14**(1): 167.

Nardi, P. M. (2018). Doing survey research: A guide to quantitative methods. New York, NY, Routledge.

Nasiruzzaman, A. B. M., *et al.* (2011). Complex network framework based dependency matrix of electric power grid. 21st Australasian Universities Power Engineering Conference (AUPEC) Brisbane, QLD, IEEE.

Nelson, D. R., *et al.* (2007). "Adaptation to environmental change: contributions of a resilience framework." Annual review of Environment and Resources **32**(1): 395.

Neuman, W. L. (2014). Basics of social research: Qualitative and quantitative approaches. Harlow, UK, Pearson Education.

Neureuther, B. D. and G. Kenyon (2009). "Mitigating supply chain vulnerability." Journal of marketing channels **16**(3): 245-263.

Newberry, M. E. (2014). "Maritime critical infrastructure cyber risk." Coast Guard Journal of Safety & Security at Sea, Proceedings of the Marine Safety & Security Council **71**(4).

Newman, L. and A. Dale (2005). "Network structure, diversity, and proactive resilience building: a response to Tompkins and Adger." Ecology and society **10**(1).

Ng, A., *et al.*, Eds. (2016). Climate Change and Adaptation Planning for Ports. London, UK, Routledge.

Ng, A. K., *et al.* (2013b). "Institutions, bureaucratic and logistical roles of dry ports: The Brazilian experiences." Journal of Transport Geography **27**: 46-55.

Ng, A. K. Y., *et al.* (2013a). "Climate Change and the Adaptation Strategies of Ports: The Australian Experiences." Research in Transportation Business & Management **8**: 186-194.

Nielsen, P. A. (2012). Collaborative coding of qualitative data, Available online at https://www.researchgate.net/publication/261633642. Kristiansand, Norway, University of Agder.

Noble, H. and J. Smith (2015). "Issues of validity and reliability in qualitative research, Available online at http://ebn.bmj.com/content/18/2/34." Evidence-Based Nursing **18**: 34-35.

Norris, F. H., *et al.* (2008). "Community resilience as a metaphor, theory, set of capacities, and strategy for disaster readiness." American journal of community psychology **41**(1-2): 127-150.

Nott, J. (2018). "The influence of tropical cyclones on long-term riverine flooding; examples from tropical Australia." Quaternary Science Reviews **182**: 155-162.

Notteboom, E. T. and W. Winkelmans (2004). Overall Market Dynamics and Their Influence on the Port Sector. Factual Report - Work Package 1 (FR-WP1). Brussels, Belgium, European Sea Ports Organisation (ESPO).

Notteboom, T. and J.-P. Rodrigue (2005). "Port Regionalisation: Towards a New Phase in Port Development." Maritime Policy & Management **32**(3): 297-313.

Notteboom, T. E. (2010). "Concentration and the Formation of Multi-port Gateway Regions in the European Container Port System: An Update." Journal of Transport Geography **18**(4): 567-583.

Notteboom, T. E., *et al.*, Eds. (2009). Ports in Proximity: Competition and Coordination among Adjacent Seaports. Aldershot, UK, Ashgate.

Notteboom, T. E. and J.-P. Rodrigue (2007). Re-assessing Port-hinterland Relationships in the Context of Global Commodity Chains. Ports, Cities, and Global Supply Chains J. Wang, D. Olivier, T. E. Notteboom and B. Slack. Aldershot, England, Ashgate Publishing, Ltd.

NRC (2011). Review of the Department of Homeland Security's Approach to Risk Analysis, Available online at https://www.fema.gov/pdf/government/grant/2011/fy11_hsgp_risk.pdf. Washington, DC, National Research Council.

NTC (2011) National Ports Strategy. National Transport Policy.

Nyborg, K., et al. (2016). "Social norms as solutions." Science **354**(6308): 42-43.

O'Connell, D., *et al.* (2016). Designing projects in a rapidly changing world: Guidelines for embedding resilience, adaptation and transformation into sustainable development projects. (Version 1.0). Washington, DC, Global Environment Facility.

Obrist, B., *et al.* (2010). "Multi-layered social resilience: a new approach in mitigation research." Progress in Development Studies **10**(4): 283-293.

O'Donnell, K. (2013). "Critical infrastructure resilience: resilience thinking in Australia's federal critical infrastructure protection policy." Salus Journal **1**(3): 13.

OECD (2017). Boosting Resilience through Innovative Risk Governance. OECD Reviews of Risk Management Policies. Paris, France, Organisation for Economic Co-operation and Development

OEM (2005). Emergency Management Act 2005, Available online at http://www8.austlii.edu.au/cgi-bin/viewdb/au/legis/wa/consol_act/ema2005190/. Perth, Western Australia Government.

O'Hare, P., *et al.* (2016). "Insurance as maladaptation: resilience and the 'business as usual' paradox." Environment and Planning C: Government and Policy **34**(6): 1175-1193.

Oliva, S. and L. Lazzeretti (2017). "Adaptation, adaptability and resilience: the recovery of Kobe after the Great Hanshin Earthquake of 1995." European Planning Studies **25**(1): 67-87.

Ongkowijoyo, C. S. and H. Doloi (2018). "Understanding of Impact and Propagation of Risk based on Social Network Analysis." Procedia Engineering **212**: 1123-1130.

Onwuegbuzie, A. J. and J. P. Combs (2011). "Data analysis in mixed research: A primer." International Journal of Education **3**(1): 13.

Onyeji, I., *et al.* (2014). "Cyber security and critical energy infrastructure." The Electricity Journal **27**(2): 52-60.

Ormston, R., *et al.* (2014). The foundations of qualitative research. Qualitative research practice: A guide for social science students and researchers. J. Ritchie, J. Lewis, C. McNaughton Nicholls and R. Ormston. London, UK, Sage**:** 1-26.

Ott, R. L. and M. Longnecker (2016). Using surveys and experimental studies to gather data. An introduction to statistical methods and data analysis. R. L. Ott and M. Longnecker. Boston, MA, Cengage Learning**:** 16-48.

Ouyang, M. (2014). "Review on modelling and simulation of interdependent critical infrastructure systems." Reliability Engineering & System Safety **121**: 43-60.

Owen, C., *et al.* (2016). "Values and Complexities in Assessing Strategic-Level Emergency Management Effectiveness." Journal of Contingencies and Crisis Management **24**(3): 181-190.

Owen, C. and P. Hayes (2017). Human factors in emergency management. Human factors challenge in emergency management: Enhancing individual and team performance in fire and emergency services. Farnham, UK, Ashgate Publishing. **1**.

P. Alcantara, P., *et al.* (2017). BCI supply chain resilience report. Berkshire, UK, Business Continuity Institute.

Paixão, A. C. and P. B. Marlow (2003). "Fourth Generation Ports - A Question of Agility?" International Journal of Physical Distribution & Logistics Management, **33**(4): 355 - 376.

Pallant, J. (2016). SPSS survival manual: A step by step guide to data analysis using IBM SPSS. New York, NY, Open University Press, Maidenhead.

Pallis, A. A. and P. Kladaki (2016). Port collaboration beyond proximity: Inter-organizational relationships of port management entities. IAME Conference 2016, 23-26 August Hamburg, Germany, PortEconomics.eu

Panayides, P. M. (2017). Global supply chain integration and competitiveness of port terminals. Ports, cities, and global supply chains. J. Wang, D. Olivier, T. Notteboom and B. Slack. Aldershot, UK, Ashgate**:** 43-56.

Pannucci, C. J. and E. G. Wilkins (2010). "Identifying and avoiding bias in research." Plastic and reconstructive surgery **126**(2): 619-625.

Pant, R., *et al.* (2014). "Stochastic measures of resilience and their application to container terminals." Computers & Industrial Engineering **70**: 183-194.

Parker, B., *et al.* (2009). Geography for Australian Citizens. Melbourne, Victoria, Macmillan Education.

Parker, R. (2010). Managing for Resilience. Resilience and Transformation: Preparing Australia for Uncertain Futures. S. Cork. Collingwood, Victoria, Australia, CSIRO Publishing.

Parkes, J. (1998). The Harbourmaster's Responsibility to Provide a Safe Port. The Work of the Harbourmaster: A Practical Guide. P. Bell. London, UK, The Nautical Institute.

Parsons, M. and P. Morley (2017). "The Australian natural disaster resilience index." Australian Journal of Emergency Management, The **32**(2): 20.

Paté-Cornell, E. and L. A. Cox (2014). "Improving risk management: from lame excuses to principled practice." Risk analysis **34**(7): 1228-1239.

Paté-Cornell, M., *et al.* (2018). "Cyber Risk management for critical infrastructure: a risk analysis model and three case studies." Risk analysis **38**(2): 226-241.

Paté-Cornell, M. E. (1996). "Uncertainties in risk analysis: Six levels of treatment." Reliability Engineering & System Safety **54**(2-3): 95-111.

Pateman, H. A. (2015). The role of strategic intent in collaboration: knowledge creation and transfer in the Australian logistics industry: part A. Australian Maritime College. Launceston, Tasmania, University of Tasmania.

Paton, D., *et al.* (2006). Exploring the complexity of social and ecological resilience to hazards. Springfield, Illinois, Charles C Thomas Publisher.

Patton, M. Q. (2015). Qualitative research and methods: Integrating theory and practice. London, UK, Sage Publications Ltd.

Pelling, M. (2011). Adaptation to climate change: from resilience to transformation. Abingdon, UK, Routledge.

Perera, T. and D. Higgins (2017). Theoretical overview of known, unknown and unknowable risks for property decision makings. 23rd Annual Pacific Rim Real Estate Society Conference, 15th – 18th January. Sydney, New South Wales, Australia. RMIT University.

Pernick, M. S. (2014). Diseases in motion. A Companion to World History. D. Northrop. Chichester, UK Wiley**:** 365-374.

Perrow, C. (2011). Normal Accidents: Living with High-Risk Technologies. Princeton, New Jersey, Princeton University Press.

Pescaroli, G. and D. Alexander (2016). "Critical infrastructure, panarchies and the vulnerability paths of cascading disasters." Natural Hazards **82**(1): 175-192.

Peterson, H. C., *et al.* (2001). "Strategic Choice along the Vertical Coordination Continuum." The International Food and Agribusiness Management Review **4**(2): 149-166.

Petroni, R., *et al.* (2004). Response rates and nonresponse in BLS and Census Bureau establishment surveys. Proceedings of the Survey Research

Methods Section, American Statistical Association, Washington, D.C, U.S. Census Bureau

Pettersen, K. A. and P. R. Schulman (2016). "Drift, adaptation, resilience and reliability: toward an empirical clarification." Safety Science.

Pettit, S. J. and A. K. C. Beresford (2005). "Emergency Relief Logistics: An Evaluation of Military, Non-military and Composite Response Models." International Journal of Logistics: Research and Applications **8**(4): 313-331.

Pettitt, T. M. (2014). The corporatized Australian port system: are there legislative constraints upon the effective operation of the model? Macquarie Graduate School of Management. Sydney, NSW, Macquarie University. PhD Thesis.

Phillips, J. (2014). Boat arrivals in Australia: A quick guide to the statistics, Available online at https://www.aph.gov.au/About_Parliament/Parliamentary_Departments/Parliamentary_Library/pubs/rp/rp1314/QG/BoatArrivals. Research Papers 2013-14. Canberra, ACT, Parliament of Australia.

Phillips, J. D., *et al.* (2015). "Graph theory in the geosciences." Earth-Science Reviews **143**: 147-160.

PIANC (2014). Harbour approach channels: design guidelines. Brussels, Belgium, Permanent International Association of Navigation Congresses - World Association for Waterborne Transport Infrastructure.

Piening, E. P. (2013). "Dynamic capabilities in public organizations." Public Management Review **15**(2): 209-245.

Pigna, F. (2014). Port authority corporatisation: Leading towards their privatisation. Port infrastructure finance. H. Meersman, E. Van de Voorde and T. Vanelslander. Abingdon, UK, Informa Law - Routledge**:** 69-86.

Pitilakis, K., *et al.* (2016). "Systemic Vulnerability and Risk Assessment of Transportation Systems Under Natural Hazards Towards More Resilient and Robust Infrastructures." Transportation Research Procedia **14**: 1335-1344.

Polemi, N. and S. Papastergiou (2017). Assessing the Risk of Ports and Their Supply Chains: The CYSM, MEDUSA, and MITIGATE Approaches. Handbook of Cyber-Development, Cyber-Democracy, and Cyber-Defense. E. G. Carayannis, D. F. J. Campbell and M. P. Efthymiopoulos. Cham, Switzerland, Springer International Publishing**:** 1-29.

Pollitt, C. and G. Bouckaert (2017). Public Management Reform: A Comparative Analysis-Into the Age of Austerity. Oxford, UK, Oxford University Press.

POM (2018). Safety and environment management plan (SEMP). Melbourne, VIC, Port of Melbourne.

Ponomarov, S. (2012). Antecedents and consequences of supply chain resilience: a dynamic capabilities perspective. Knoxville, TN, University of Tennessee.

Ports (2017). "Australian ports industry." 2017, from http://www.portsaustralia.com.au/.

Ports (2018). "Work undertaken." Retrieved 7 January 2018, from http://www.portsaustralia.com.au/about/work-undertaken/.

Power, M. (2007). Organized uncertainty: Designing a world of risk management. Oxford, UK, Oxford University Press on Demand.

Power, M. (2009). "The risk management of nothing." Accounting, organizations and society **34**(6-7): 849-855.

PPIAF (2016). Port Reform Tool Kit. Washington, DC, World Bank: Public – Private Infrastructure Advisory Facility.

Prentice, B. E. (2003a). Importance of Intermodal Connectivity and Bottleneck Elimination. Proceedings of the 38th Annual Conference of the Canadian Transportation Research Forum: Crossing Borders (CTRF) May 11-14. Ottawa, Ontario.

Presser, S., *et al.* (2004). "Methods for testing and evaluating survey questions." Public Opinion Quarterly **68**(1): 109-130.

Price, W. T., *et al.* (1983). A research agenda for seaport management and related maritime transport issues. Los Angeles, CA, University of Southern California.

Price, W. T. and A. Hashemi (2015). Seaport operations and security. Securing Transportation Systems. S. Hakim, G. Albert and Y. Shiftan. Hoboken, NJ, John Wiley**:** 233-255.

Proença, D., *et al.* (2017). Risk Management: A Maturity Model Based on ISO 31000. IEEE 19th Conference on Business Informatics (CBI), Universidade de Lisbon, Lisbon, Portugal, IEEE.

Puig, M., *et al.* (2014). "Identification and selection of environmental performance indicators for sustainable port development." Marine pollution bulletin **81**(1): 124-130.

Purdy, G. (2010). "ISO 31000: 2009—setting a new standard for risk management." Risk analysis **30**(6): 881-886.

Pye, G. and M. Warren (2007). "Modelling critical infrastructure systems." Journal of information warfare **6**(1): 41-53.

QLD (2017). A Guide to Risk Management, Available online at https://www.treasury.qld.gov.au/resource/guide-risk-management/. Q. Treasury. Brisbane, QLD, Queensland Government.

QSA (2013). Ports Sector Retention and Disposal Schedule. Q. S. Archives. Brisbane, QLD, Queensland Government.

Quéro, Y.-C. and B. Benoît Dupont (2017). "Nodal governance: toward a better understanding of node relationships in local security governance." Policing and Society, An International Journal of Research and Policy **27**: 1-19.

Quigley, K. and K. Porter (2016). Risk Refined at the Science–Policy Interface: The International Risk Governance Framework Applied to Different Classes of Coastal Zone Risks. Science, Information, and Policy Interface for Effective Coastal and Ocean Management. B. H. MacDonald, S. S. Soomai, E. M. De Santo and P. G. Wells. Boca Raton, FL, CRC Press**:** 103.

Qureshi, Z. H. (2007). A Review of Accident Modelling Approaches for Complex Socio-Technical Systems. 12th Australian Workshop on Safety Related Programmable Systems (SCS'07), Adelaide.

Rademaker, L. L., *et al.* (2012). "Using computer-assisted qualitative data analysis software (CAQDAS) to re-examine traditionally analyzed data: Expanding our understanding of the data and of ourselves as scholars." The Qualitative Report **17**(22): 1.

Ramos, S. J. (2017). "Resilience, Path Dependence, and the Port: The Case of Savannah." Journal of Urban History: 0096144217704183.

Ravitch, S. M. and M. Riggan (2016). Reason & rigor: How conceptual frameworks guide research. Los Angeles, CA, Sage Publications.

RDA (2018). National Network, Available online at https://rda.gov.au/files/rda_map_national.pdf. Canberra, ACT, Department of Infrastructure, Regional Development and Cities - Regional Development Australia.

Reason, J. (1998). "Achieving a Safe Culture: Theory and Practice." Work & Stress **12**(3): 293-306.

Reason, J. (2008). Managing the Risks of Organisational Accidents. Aldershot UK, Ashgate Publishing Ltd.

Reason, J. (2016). Managing the Risks of Organizational Accidents. Abingdon, UK, Routledge.

Ren, S. (2017). Scholar-Practitioners in HRD: A Qualitative Study of Research-Practice Integration.

Renn, O. (2014). A generic model for risk governance: Concept and application to technological installations. Risk Governance of Offshore Oil and Gas Operations. P. H. Lindøe, M. Baram and R. O. New York, NY, Cambridge University Press

Renn, O. (2017). Risk governance: coping with uncertainty in a complex world. London, UK, Routledge.

Renn, O. and A. Klinke (2015). Risk Governance and Resilience: New Approaches to Cope with Uncertainty and Ambiguity. Risk Governance: The Articulation of Hazard, Politics and Ecology. U. Fra.Paleo. Dordrecht, Springer Netherlands**:** 19-41.

Rey, H. (2015). Dilemma not trilemma: the global financial cycle and monetary policy independence. Cambridge, MA, National Bureau of Economic Research.

Reynolds, Z. (2017). Cyclone shuts down Australian coal ports. Fairplay. London, UK, IHS Fairplay.

Reynolds, G. (2010). The possible future market challenges for relevant ports. Background Paper 5 for the National Ports Strategy. Melbourne, VIC, Infrastructure Australia and the National Transport Commission.

Rice, J. (2003). Supply Chain Response to Terrorism: Creating Resilient and Secure Supply Chains. Supply Chain Response to Terrorism Project. Y. Sheffi. Massachusetts, US, MIT Center for Transportation and Logistics**:** 1-59.

Rice, J. B. and K. Trepte (2012). The MIT CTL Port Resilience Survey Report, Available online at http://ctl.mit.edu/sites/ctl.mit.edu/files/Port%20resilience%20survey%20report%20v27%20sans%20SEM.pdf. Cambridge, Massachusetts US, MIT Center for Transportation & Logistics.

Rinaldi, S. M. (2004). Modelling and simulating critical infrastructures and their interdependencies. 37th annual Hawaii international conference on system sciences 2004. Big Island, Hawaii, IEEE**:** 8 pp.

Rindfuss, R. R., *et al.* (2015). "Do low survey response rates bias results? Evidence from Japan." Demographic Research **32**: 797.

Ritchie, J., *et al.*, Eds. (2013). Qualitative research practice: A guide for social science students and researchers. London, UK, Sage.

Robbins, M. and D. Smith (2000). PD 6668 Managing Risk for Corporate Governance. London, UK, British Standards Institution.

Roberts, C. M. (2006). "Radio Frequency Identification (RFID)." Computers & Security **25**(1): 18-26.

Roberts, N. C. (2000). "Wicked problems and network approaches to resolution." International Public Management Review **1**: 1-19.

Robinson, C. and D. Shewitz (2017). Understanding Low-Probability/High-Consequence Events. ASSE Professional Development Conference and Exposition, Denver, Colorado, American Society of Safety Engineers.

Robinson, R. (2002). "Ports as Elements in Value-Driven Chain Systems: The New Paradigm." Maritime Policy & Management **29**: 241-255.

Robinson, R. M., *et al.* (2013). Risk and reliability: Engineering due diligence. Melbourne, VIC, R2A Pty Ltd.

Rodrigue, J.-P., *et al.* (2009). The Geography of Transport Systems. Abingdon, UK, Routledge.

Rodrigue, J.-P. and T. Notteboom (2017). Re-assessing port-hinterland relationships in the context of global commodity chains. Ports, cities, and global supply chains. J. Wang, D. Olivier, T. Notteboom and B. Slack. Aldershot, UK, Ashgate**:** 67-82.

Rodriguez, P., *et al.* (2002). Corrupt governments matter: How corruption affects the entry strategies of multinationals. College Station, Texas, Texas A&M University.

Rogelberg, S. G. and J. M. Stanton (2007). Introduction: Understanding and dealing with organizational survey nonresponse. Los Angeles, CA, Sage Publications

Rogers, P. (2011). "Development of resilient Australia: enhancing the PPRR approach with anticipation, assessment and registration of risks." Australian Journal of Emergency Management, The **26**(1): 54.

Rondinelli, D. and M. Berry (2000). "Multimodal transportation, logistics, and the environment: managing interactions in a global economy." European Management Journal **18**(4): 398-410.

Ronza, A., *et al.* (2003). "Predicting the Frequency of Accidents in Port Areas by Developing Event Trees from Historical Analysis." Journal of Loss Prevention in the Progress of Industries **16**: 551-560.

Rose, A. (2017). Economic Resilience to Terrorism and Natural Hazards. Improving Homeland Security Decisions. A. E. Abbas, M. Tambe and D. von Winterfeldt. Cambridge, UK., Cambridge University Press**:** 193.

Rose, A. and C. K. Huyck (2016). "Improving catastrophe modelling for business interruption insurance needs." Risk analysis **36**(10): 1896-1915.

Rose, A. and D. Wei (2013). "Estimating the Economic Consequences of a Port Shutdown: The Special Role of Resilience." Economic Systems Research **25**(2): 212-232.

Rose, A., *et al.* (2017). Economic Consequences of and Resilience to a Disruption of Petroleum Trade: The Role of Seaports in US Energy Security. Los Angeles, CA, University of Southern California.

Rose, A. Z. (2009). "A framework for analyzing the total economic impacts of terrorist attacks and natural disasters." Journal of Homeland Security and Emergency Management **6**(1).

Rosenhead, J. (1998). Complexity Theory and Management Practice. Operational Research Working Papers, LSEOR 98.25. London, UK, London School of Economics and Political Science.

Rosenoer, J. and W. Scherlis (2007). "Risk gone wild." Harvard Business Review **87**(5): 26.

Rosenthal, U., *et al.* (2001). The changing world of crises and crisis management. Springfield, Illinois, Charles C Thomas.

Roth, A. and E. Nakashima (2017). Massive cyberattack hits Europe with widespread ransom demands, Available online at https://www.washingtonpost.com/world/europe/ukraines-government-key-infrastructure-hit-in-massive-cyberattack/2017/06/27/7d22c7dc-5b40-11e7-9fc6-c7ef4bc58d13_story.html. Washington Post, Washington, DC, Ryan, F.

Rotimi, J. O. B. (2010). An examination of improvements required to legislative provisions for post disaster reconstruction in New Zealand. Canterbury, New Zealand, University of Canterbury.

Royds, D., *et al.* (2005). "A case study in forensic chemistry: The Bali bombings." Talanta **67**(2): 262-268.

Rubin, C. B. (1998). What hazards and disasters are likely in the 21st century-or sooner? Denver, CO, Natural Hazards Research and Applications Information Center, University of Colorado.

Rubin, C. B. (2004). Emergency Management in the 21st Century: Dealing with Al Qaeda, Tom Ridge, and Julie Gerberding. Boulder, CO, University of Colorado - Natural Hazards Research and Applications Information Center.

Rudestan, K. E. and R. R. Newton (2015). Surviving Your Dissertation: A Comprehensive Guide to Content and Process. Sage.

Ruiz-Martin, C., *et al.* (2017). The Application of the Viable System Model to Enhance Organizational Resilience. Advances in Management Engineering. A. López-Paredes. Cham, Switzerland, Springer**:** 95-107.

Russell, R. C., *et al.* (2009). "Dengue and climate change in Australia: predictions for the future should incorporate knowledge from the past." Medical Journal of Australia **190**: 265-268.

Sadgrove, K. (2016). The complete guide to business risk management. Abingdon, UK, Routledge.

Sahebjamnia, N., *et al.* (2017). "Building organizational resilience in the face of multiple disruptions." International Journal of Production Economics **197**: 63-83.

Saisana, M. and F. Cartwright (2007). Composite indicators: Science or artefacts. Biannual Conference. Prague, Czech Republic, European Survey Research Association.

Sakalayen, Q. M. H., *et al.* (2016). "Investigating the strategies for Australian regional ports' involvement in regional development." International Journal of Shipping and Transport Logistics **8**(2): 153-174.

Salmon, P., *et al.* (2011). "Coordination during multi-agency emergency response: issues and solutions." Disaster Prevention and Management: An International Journal **20**(2): 140-158.

Sanchez-Rodrigues, V., *et al.* (2009). Diagnosis of 'Extra Distance' in the UK FMCG Primary Transport Sector. 14th Annual Logistics Research Network Conference, 9th – 11th September, Cardiff, Wales.

Scandizzo, S. (2005). "Risk mapping and key risk indicators in operational risk management." Economic Notes **34**(2): 231-256.

Scanlon, J. (1996). "Help from the deep: the potential of ocean-based response to disaster." Disaster Prevention and Management: An International Journal **5**(3): 16-23.

Schein, E. H. (1996). "Three Cultures of Management: The Key to Organizational Learning." Sloan Management Review **38**(1): 9-20.

Schiffino, N., *et al.* (2017). "Post-crisis learning in public agencies: what do we learn from both actors and institutions?" Policy Studies **38**(1): 59-75.

Schiller, F. and G. Prpich (2014). "Learning to organise risk management in organisations: What future for enterprise risk management?" Journal of Risk Research **17**(8): 999-1017.

Schipper, E. L. F. and L. Langston (2015). A comparative overview of resilience measurement frameworks. London, UK, Overseas Development Institute.

Schnaubelt, C. M., *et al.* (2014). Vulnerability Assessment Method Pocket Guide: A Tool for Center of Gravity Analysis. Washington, DC, RAND Corporation.

Schoenbaum, T. (2016). Admiralty and Maritime Law. St Paul, MN, West Academic.

Schutt, R. K. (2014). Investigating the social world: The process and practice of research. Canada, Sage Publications.

Scolobig, A., *et al.* (2015). "Towards people-centred approaches for effective disaster risk management: Balancing rhetoric with reality." International Journal of Disaster Risk Reduction **12**: 202-212.

Seager, T. P., *et al.* (2016). Resilience and Risk: Redesigning resilient infrastructure research. NATO Advanced Research Workshop on Resilience-Based Approaches to Critical Infrastructure Safeguarding, 26-29 June, Azores, Portugal, Springer.

Sekaran, U. and R. Bougie (2016). Research methods for business: A skill building approach. Chichester, UK, John Wiley & Sons.

Seville, E., Ed. (2009). Resilience: great concept but what does it mean for organizations? Community Resilience: Research, Planning and Civil Defense Emergency Management. Wellington, NZ, Ministry of Civil Defense & Emergency Management.

Shafieezadeh, A. and L. I. Burden (2014). "Scenario-based resilience assessment framework for critical infrastructure systems: Case study for seismic resilience of seaports." Reliability Engineering & System Safety **132**: 207-219.

Shaw, D. R., *et al.* (2017). "Multi-level port resilience planning in the UK: How can information sharing be made easier?" Technological Forecasting and Social Change **121**: 126-138.

Shaw, D. R., *et al.* (2014). "The paradox of social resilience: How cognitive strategies and coping mechanisms attenuate and accentuate resilience." Global environmental change **25**: 194-203.

Sheehan, T. (2013). Tenth anniversary: Trusted information sharing network for critical infrastructure resilience 2013. Critical Infrastructure and Protective Security Policy Branch. Canberra, ACT, Australian Government**:** 24.

Sheffi, Y. (2007). The resilient enterprise: Overcoming vulnerability for competitive advantage. Cambridge, Massachusetts, MIT Press.

Sheffi, Y. (2017). The Power of Resilience: How the Best Companies Manage the Unexpected. Cambridge, Massachusetts, MIT Press.

Shefrin, H. (2016a). Behavioral Risk Management: Managing the Psychology that Drives Decisions and Influences Operational Risk. Basingstoke, Hampshire UK, Palgrave MacMillan.

Shefrin, H. (2016b). "Behavioural insights for improving the practice of risk management." Journal of Risk Management in Financial Institutions **9**(2): 112-119.

Shemmings, D. and I. T. Ellingsen (2012). Using Q methodology in qualitative interviews. A. F. Gubrium, J. A. Holstein, A. B. Marvasti and K. D. McKinney. Thousand Oaks, CA, Sage Publications.

Shields, P. M. and N. Rangarajan (2013). A playbook for research methods: Integrating conceptual frameworks and project management. Stillwater, OK, New Forums Press.

Shiller, R. J. (2009). The new financial order: Risk in the 21st century. Princeton, NJ, Princeton University Press.

Short, D. C. and T. J. Shindell (2009). "Defining HRD scholar-practitioners." Advances in Developing Human Resources **11**(4): 472-485.

Shrivastava, S., *et al.* (2009). "Normal accident theory versus high reliability theory: A resolution and call for an open system view of accidents." Human relations **62**(9): 1357-1390.

Sierra, J. P., *et al.* (2017). "Modelling the impact of climate change on harbour operability: The Barcelona port case study." Ocean Engineering **141**: 64-78.

Simpson, J., Ed. (2018). Oxford Dictionary of English. Oxford, UK, Oxford University Press.

Simsek, Z. and J. F. Veiga (2001). "A primer on internet organizational surveys." Organizational research methods **4**(3): 218-235.

Singh, A., *et al.* (2016). "Understanding the port-centric logistics clusters: Concepts, characteristics." Innovative Solutions for Implementing Global Supply Chains in Emerging Markets: 257.

Singh, N. (2008) The Charterers' Safe Port Obligation: Total Immunity. Publications

Siniscalco, M. T. and N. Auriat (2005). Questionnaire design. Quantitative research methods in educational planning. Paris, France, UNESCO International Institute for Educational Planning**:** 1-92.

Smith, D. and A. Irwin (2006). "Complexity, Risk and Emergence: Elements of a" Management" Dilemma." Risk Management **8** 221-226.

Smith, A. B. and R. W. Katz (2013). "US billion-dollar weather and climate disasters: data sources, trends, accuracy and biases." Natural hazards **67**(2): 387-410.

Smithson, M. (2010). Ignorance and Uncertainty. Tackling Wicked Problems Through the Transdisciplinary Imagination. V. A. Brown, J. A. Harris and J. Y. Russell. London, UK, Earthscan Ltd.

Smythe, T. C. (2013). Assessing the impacts of Hurricane Sandy on the Port of New York and New Jersey's Maritime responders and response infrastructure. Quick Response Report No. 238: Final Report to the University of Colorado Natural Hazards Center, Natural Hazards Center.

Sobel, P. J. and K. F. Reding (2004). "Aligning corporate governance with enterprise risk management." Management Accounting Quarterly **5**(2): 29.

Solecki, W., *et al.* (2017). "Transitions between risk management regimes in cities." Ecology and Society **22**(2).

Song, D. W. and P. M. Panayides (2007). Global Supply Chain and Port/Terminal: Integration and Competitiveness International Conference on Logistics, Shipping and Port Management, 29-30 March Taiwan.

Song, D. W. and F. Parola (2014). "Strategizing Port Logistics Management and Operations for Value Creation in Global Supply Chains." International Journal of Logistics: Research and Applications, **18**(Special Issue): 1.

Song, D. W. and P. M. Panayides (2012). Maritime Logistics: A Complete Guide to Effective Shipping and Port Management. London, UK, Kogan-Page.

Songhurst, B. (2014). LNG plant cost escalation. Oxford Institute for Energy Studies. Oxford, UK, University of Oxford.

Sookhak, M., *et al.* (2017). "Dynamic remote data auditing for securing big data storage in cloud computing." Information Sciences **380**: 101-116.

Sookhak, M., *et al.* (2017). "Attribute-based data access control in mobile cloud computing: Taxonomy and open issues." Future Generation Computer Systems **72**: 273-287.

Southwick, F. S., *et al.* (2017). Leadership and resilience. Leadership today: Practices for Personal and Professional Performance. Switzerland, Springer International Publishing**:** 315-333.

Southworth, F., *et al.* (2014). Making US Ports Resilient as Part of Extended Intermodal Supply Chains. Washington, DC, National Academy of Sciences - Transportation Research Board.

Sporleder, T. L. (2006). Strategic Alliances and Networks in Supply Chains. Quantifying the Agri-food Supply Chain. C. J. M. Ondersteijn, J. H. M. Wijnands, R. B. M. a. Huirne and O. van Kooten. Dordrecht, The Netherlands, Springer.

Srikanth, S. N. and R. Venkataraman (2013). Strategic Risk Management in Ports. Risk Management in Port Operations, Logistics and Supply Chain Security. K. Bichou, M. Bell and A. Evans. London, Informa Law**:** 335-345.

St Germain, S. W., *et al.* (2014). Guidelines for implementation of an advanced outage control center to improve outage coordination, problem resolution, and outage risk management. Idaho Falls, ID, U.S. Department of Energy National Laboratory - Idaho National Lab.

Stacey, R. D. (1993). Strategic Management and Organisational Dynamics. London, UK, Pitman.

Stacey, R. D. (2007). Strategic Management and Organisational Dynamics: The Challenge of Complexity to Ways of Thinking about Organisations. New Jersey, Financial Times Prentice Hall.

Stažnik, A., *et al.* (2017). "Identification and analysis of risks in transport chains." Journal of Applied Engineering Science **15**(1): 61-70.

Steele, W., *et al.* (2017). "What's critical about critical infrastructure?" Urban Policy and Research **35**(1): 74-86.

Stenek, V., *et al.* (2011). Climate risk and business: Ports. Washington, DC, International Finance Corporation 1-190.

Stephenson, A. (2010). Benchmarking the resilience of organisations Civil and Natural Resources Engineering Department Christchurch, New Zealand, University of Canterbury, PhD Thesis.

Stephenson, A., *et al.* (2010). "Measuring and comparing organisational resilience in Auckland." Australian Journal of Emergency Management, The **25**(2): 27.

Stirling, A. (2007). "Risk, precaution and science: towards a more constructive policy debate." EMBO Reports **8**(4): 309-315.

Stopford, M. (2013). Maritime economics. Abingdon, UK, Routledge.

Strang, K. D., *et al.* (2018). Research, practices, and innovations in global risk and contingency management. Hershey, PA, IGI Global.

Straube, F., *et al.* (2010). Trends and Strategies in Global Logistics: New Directions in Supply Chain Management. C. D. J. Waters. London, UK, Kogan Page.

Stulz, R. M. (2008). "Risk management failures: What are they and when do they happen?" Journal of Applied Corporate Finance **20**(4): 39-48.

Sujanto, F., *et al.* (2008). An Integrated Framework for Comprehensive Collaborative Emergency Management. Collaborative Decision Making:

Perspectives and Challenges. P. Zaraté. Amsterdam, The Netherlands, IOS Pres**:** 127-138.

Sunstein, C. R. and R. Zeckhauser (2011). "Overreaction to fearsome risks." Environmental and Resource Economics **48**(3): 435-449.

Suter, G. W. (2016). Ecological Risk Assessment. Boca Raton, FLA, CRC Press.

Swarbrick, B. (2012). Multivariate data analysis for Dummies. Chichester, UK, John Wiley & Sons Ltd.

Symonds, E. (2011). "A practical application of SurveyMonkey as a remote usability-testing tool." Library Hi Tech **29**(3): 436-445.

Talanquer, V. (2014). Using qualitative analysis software to facilitate qualitative data analysis. Tools of Chemistry Education Research. D. Bunce. Washington, DC, ACS Publications**:** 83-95.

Tampubolon, S. D. (2012). Innovative enterprise risk management (ERM) for the Indonesian Port Corporation: A recommendation for improving the implementation plans. Department of Industrial Engineering and Innovation Sciences. Eindhoven, The Netherlands, Eindhoven University of Technology. **MSc**.

Tan, X. M., *et al.* (2015). Economic impact of port disruptions on industry clusters: A case study of Shenzhen. Transportation Information and Safety (ICTIS), 2015 International Conference on, IEEE.

Taneja, P., *et al.* (2010). "Dealing with uncertainty in design of port infrastructure systems." Journal of Design research **8**(2): 101-118.

Tang, C. S. (2006a). "Robust Strategies for Mitigating Supply Chain Disruptions." International Journal of Logistics Research and Applications: A Leading Journal of Supply Chain Management **9**(1): 33-45.

Tang, C. S. (2006b). "Perspectives in Supply Chain Risk Management." International Journal of Production Economics **103**: 451–488.

Tang, O. and S. N. Musa (2011). "Identifying risk issues and research advancements in supply chain risk management." International Journal of Production Economics **133**(1): 25-34.

Tangen, S. (2005). "Improving the performance of a performance measure." Measuring Business Excellence **9**(2): 4-11.

Tanner, A. S., *et al.* (2018). "The water Utility Adoption Model (wUAM): Understanding influences of organisational and procedural innovation in a UK water utility." Journal of Cleaner Production **171**: S86-S96.

Tarrant, M. (2010). "The organisation: risk, resilience and governance." Australian Journal of Emergency Management, The **25**(2): 13.

Tashakkori, A. and C. Teddlie (2010). Sage handbook of mixed methods in social & behavioral research. Los Angeles, CA, Sage.

Tavakol, M. and R. Dennick (2011). "Making sense of Cronbach's alpha." International journal of medical education **2**: 53.

Teddlie, C. and A. Tashakkorie (2009). Foundations of mixed methods research: Integrating quantitative and qualitative approaches in the social and behavioural sciences. Thousand Oaks, CA Sage.

Teddlie, C. and F. Yu (2007). "Mixed methods sampling: A typology with examples." Journal of mixed methods research **1**(1): 77-100.

Teece, D., *et al.* (2016). "Dynamic capabilities and organizational agility: Risk, uncertainty, and strategy in the innovation economy." California Management Review **58**(4): 13-35.

Teece, D. J. (2007). "Explicating dynamic capabilities: the nature and microfoundations of (sustainable) enterprise performance." Strategic management journal **28**(13): 1319-1350.

Teece, D. J. (2017a). "Business models and dynamic capabilities." Long range planning **51**: 40-49.

Teece, D. J. (2017b). Dynamic capabilities and the multinational enterprise. Globalization: Strategies and effects. B. J. Christensen and C. Kowalczyk. Berlin, Germany Springer-Verlag 105-129.

Teece, D. J. (2018). "Dynamic capabilities as (workable) management systems theory 1." Journal of Management & Organization: 1-10.

Teece, D. J., *et al.* (1997). "Dynamic capabilities and strategic management." Strategic management journal **18**(7): 509-533.

Tekathen, M. and N. Dechow (2013). "Enterprise risk management and continuous re-alignment in the pursuit of accountability: A German case." Management Accounting Research **24**(2): 100-121.

TEMP (2015). Tasmanian Emergency Management Plan, Available online at http://www.ses.tas.gov.au/h/em/publications/temp. T. S. E. Service. Hobart, TAS, Tasmanian Government.

Thai, V. V. and S. Chen (2011). The Role of Ports in Supply Chain Disruption Management. International Conference on Free Port and International Logistics, Kainan University.

Thekdi, S. and T. Aven (2016). "An enhanced data-analytic framework for integrating risk management and performance management." Reliability Engineering & System Safety **156**: 277-287.

Thellesen, L., *et al.* (2015). "Curriculum development for a national cardiotocography education program: a Delphi survey to obtain consensus on learning objectives." Acta obstetricia et gynecologica Scandinavica **94**(8): 869-877.

Thoits, M. (2009). Enterprise Risk Management Technology Solutions, Risk and Insurance Management Society, Available online at https://www.rims.org/resources/ERM/Documents/ERM%20Technology%20Solutions.pdf. New York, NY, RIMS Technology Advisory Council.

Tilman, D. and J. A. Downing (1994). "Biodiversity and stability in grasslands." Nature **367**(6461): 363.

Tisdall, S. (2013). Fukushima nuclear disaster is warning to the world, says power company boss, Available online at https://www.theguardian.com/environment/2013/nov/19/uk-government-new-plant-fukushima-nuclear-disaster-warning D. Carrington. London, UK, The Guardian**:** [no pagination].

TISN (2015). Critical infrastructure resilience strategy. (TISN). Canberra, ACT, Commonwealth of Australia.

TISN (2016). "Trusted Information Sharing Network (TISN) for Critical Infrastructure Resilience, Available online at http://www.tisn.gov.au/Pages/default.aspx." Critical Infrastructure Resilience. 2016.

Tjoa, S. (2012). Designing business continuity response. Faculty of Computer Science. Vienna, Austria, University of Vienna.

Todd, P. (2015). "Safe port issues." Lloyd's Maritime and Commercial Law Quarterly **2015**(Part 3): 265-271.

Toscano, N. (2016). National strikes shut down docks as work tensions flare. The Age. Melbourne, Vic, Fairfax Media.

Tracey, A. (2011) The Queensland Floods, Available online at https://www.amsa.gov.au/forms-and-publications/environment/.../ONSCENE19.pdf. On Scene.

Treasury (2004). The Orange Book: Management of Risk-Principles and Concepts. European Journal of Operational Research. H. Treasury. London, UK, UK Government.

Trepte, K. and J. B. Rice Jr (2014). "An initial exploration of port capacity bottlenecks in the USA port system and the implications on resilience." International Journal of Shipping and Transport Logistics **6**(3): 339-355.

Trucco, P. and B. Petrenj (2017). Resilience of Critical Infrastructures: Benefits and Challenges from Emerging Practices and Programmes at Local Level. NATO Advanced Research Workshop on Resilience-Based Approaches to Critical Infrastructure Safeguarding, 26–29 June 2016, Azores, Portugal, Springer.

Trujillo, L. and G. Nombela (1999). Privatization and regulation of the seaport industry. Policy research working paper. Washington, DC, World Bank Publications. **2181**.

Trump, B. D., *et al.* (2017). Social Resilience and Critical Infrastructure Systems. Resilience and Risk, NATO Science for Peace and Security Series C: Environmental Security. I. Linkov and J. M. Palma-Oliveira. Amsterdam, the Netherlands, IOS.

Tsinker, G. P., Ed. (2004). Port Engineering: Planning, Construction, Maintenance, and Security. Hoboken, New Jersey, John Wiley & Sons.

Tsinker, G. P. (2014). Handbook of port and harbor engineering: geotechnical and structural aspects, Springer.

Tucci, A. E. (2017). Cyber risks in the marine transportation system. Cyber-Physical Security. Cham, Switzerland, Springer. **3:** 113-131.

Tyler, S., *et al.* (2014). Developing indicators of urban climate resilience, Available online at http://i-s-e-t.org/resources/working-papers/wp2-climate-resilience.html, ISET Climate Resilience Working Paper.

Ummenhofer, C. C. and G. A. Meehl (2017). "Extreme weather and climate events with ecological relevance: a review." Philosophical Transactions of the Royal Society of London B – Special issue 9 on "Behavioural,

ecological and evolutionary responses to extreme climatic events" **372**(1723): 20160135.

UNCTAD (2017). Review of Maritime Transport 2017. D. Barki and L. Délèze-Black. Geneva, Switzerland., United Nations Conference on Trade and Development.

UNISDR (2015). Sendai Framework for Disaster Risk Reduction 2015-2030, Available online at www.unisdr.org/we/inform/publications/43291. Geneva, Switzerland, United Nations Office for Disaster Risk Reduction.

Urdan, T. C. (2017). Statistics in plain English. New York, NY, Taylor & Francis.

Urlainis, A., *et al.* (2014). "Damage in Critical Infrastructures Due to Natural and Man-made Extreme Events – A Critical Review." Procedia Engineering **85**: 529-535.

Vacha-Haase, T. and B. Thompson (2011). "Score reliability: A retrospective look back at 12 years of reliability generalization studies." Measurement and Evaluation in Counseling and Development **44**(3): 159-168.

Van de Voorde, E. and W. Winkelmans (2002). Conclusions and policy implications. Port competitiveness: an economic and legal analysis of the factors determining the competitiveness of seaports. Antwerp, Belgium, De Boeck Limited**:** 133-146.

Van den Berghe, K. (2015). Beyond geographic path dependencies: towards a post-structuralist approach of the port-city interface. Differences & Connections: Beyond Universal Theories in Planning, Urban, and Heritage Studies, Palermo, Italy, AESOP Young Academics Coordination Team.

Van Der Burgt, C. (1994). "Permanent International Association of Navigation Congresses (PIANC)." Marine pollution bulletin **29**(6-12): 398-400.

Van Der Vegt, G. S., *et al.* (2015). "Managing Risk and Resilience: From the Editors." Academy of Management Journal **58**(4): 971-980.

Van der Vorst, G. A. J. and A. J. M. Beulens (2002). "Identifying Sources of Uncertainty to Generate Supply Chain Redesign Strategies." International Journal of Physical Distribution & Logistics Management **32**(6): 409-430.

van Grinsven, J. H. M. (2009). Improving operational risk management. Amsterdam, The Netherlands, IOS Press.

Vanderheiden, S. (2008). "Radical environmentalism in an age of antiterrorism." Environmental Politics **17**(2): 299-318.

Verdon-Kidd, D. C., *et al.* (2016). "East Coast Lows and the Pasha Bulker storm–lessons learned nine years on." Journal of Southern Hemisphere Earth System Science: 152-161.

Viellaris, R. and P. Osborne (2017). Peter Dutton to be elevated with creation of Australian Department of Homeland Security. Brisbane Courier-Mail. Brisbane, Queensland, News Corporation.

Vilko, J., *et al.* (2012). The Nature of Risk, Visibility and Control in Supply Chains. Lappeenranta, Finland, School of Business, Lappeenranta University of Technology.

Vogus, T. J. and K. M. Sutcliffe (2007). Organizational resilience: towards a theory and research agenda. 2007 IEEE International Conference on Systems, Man and Cybernetics, 7-10 October Montreal, Canada, IEEE.

Vonck, I. and T. Notteboom (2016). "Panarchy within a port setting." Journal of Transport Geography **51**: 308-315.

Vonck, I., *et al.* (2017). Seaport competition based on structural complementarity and substitutability. Annual conference of the International Association of Maritime Economists (IAME), August 23-26. Hamburg, Germany.

Wagner, J. R. (2008). Adaptive survey design to reduce nonresponse bias, University of Michigan.

Wagner, S. M. and N. Neshat (2010). "Assessing the Vulnerability of Supply Chains using Graph Theory." International Journal of Production Economics **126**: 121-129.

Waidringer, J. and K. Lumsden (1998). Simulation and Optimisation of Port Terminals, Using a Network Concept. 8th World Conference on Transport Research. Antwerp, Belgium.

Wakeman, T. H. (2013). Lessons from Hurricane Sandy for Port Resilience, available online at http://www.utrc2.org/publications/hurricane-sandy-port-resilience. Hoboken NJ US, Stevens Institute of Technology.

Wakeman, T. H., *et al.* (2017). Governance and resilience: Challenges in disaster risk reduction. TR News.

Walker, B., *et al.* (2012). "Drivers," slow" variables," fast" variables, shocks, and resilience." Ecology and Society **17**(3).

Walker, B. and D. Salt (2012). Resilience practice: building capacity to absorb disturbance and maintain function. Washington, DC, Island Press.

Walker, W. E., *et al.* (2013). Deep uncertainty. Encyclopaedia of operations research and management science. Boston, MA, Springer**:** 395-402.

Walker, W. E., *et al.* (2010). "Addressing deep uncertainty using adaptive policies: Introduction to section 2." Technological Forecasting and Social Change **77**(6): 917-923.

Wallace, M. and L. Webber (2017). The disaster recovery handbook: A step-by-step plan to ensure business continuity and protect vital operations, facilities, and assets. New York, NY, AMACOM Div. American Mgmt. Assn.

Walsh, K. J., *et al.* (2016). "Natural hazards in Australia: storms, wind and hail." Climatic Change **139**(1): 55-67.

Wan, C., *et al.* (2017). "Resilience in transportation systems: a systematic review and future directions." Transport Reviews: 1-20.

Wang, L. (2011). "Study on Port Logistics Marketing under the Environment of Supply Chain " International Journal of Business and Management **6**(3): 267-271.

Wang, X., *et al.* (2013). "Risk Perception and Communication in International Maritime Shipping in Japan After the Fukushima Daiichi Nuclear Power Plant Disaster." Transportation Research Record: Journal of the Transportation Research Board **2330**(1): 87-94.

Ward, M. (2004). Quantifying the world: UN ideas and statistics. Bloomington, Indiana, Indiana University Press.

Wasserman, I. C. and K. E. Kram (2009). "Enacting the scholar—Practitioner role: An exploration of narratives." The Journal of Applied Behavioral Science **45**(1): 12-38.

Waters, C. D. J. (2011). Supply Chain Risk Management: Vulnerability and Resilience in Logistics. London, UK, Kogan Page.

Waugh, W. L. (2015). Living with Hazards, Dealing with Disasters: An Introduction to Emergency Management: An Introduction to Emergency Management. Abingdon, UK, Routledge.

Weeserik, B. and M. Spruit (2018). "Improving Operational Risk Management Using Business Performance Management Technologies." Sustainability **10**(3): 640.

WEF (2018). The Global Risks Report 2018: World Economic Forum Global Risks Perception Survey 2017–2018, Available online at https://www.mmc.com/content/dam/mmc-web/Global-Risk-Center/Files/the-global-risks-report-2018.pdf. Geneva, Switzerland, World Economic Forum.

Wei, D., *et al.* (2017). Evaluating the Role of Resilience in Recovering from Major Port Disruptions. Transportation Research Board 96th Annual Meeting, January 8-12: Connecting Communities with Innovative Transportation. Washington DC, Transportation Research Board

Weick, K. E. and K. M. Sutcliffe (2015). Managing the unexpected: sustained performance in a complex world. Hoboken, NJ, John Wiley & Sons.

Weitzman, E. and M. B. Miles (1995). Computer programs for qualitative data analysis. Thousand Oaks, CA, Sage.

Weitzman, E. A. (1999). "Analyzing qualitative data with computer software." Health Services Research **34**(5 Pt 2): 1241.

Welsh, M. (2014). "Resilience and responsibility: governing uncertainty in a complex world." The Geographical Journal **180**(1): 15-26.

Wendler, R. (2012). "The maturity of maturity model research: A systematic mapping study." Information and software technology **54**(12): 1317-1339.

Wendler, R. (2014). Development of the organizational agility maturity model. Computer Science and Information Systems (FedCSIS), 2014 Federated Conference on, IEEE.

Westrum, R. (2006). A Typology of Resilience Situations. Resilience Engineering: Concepts and Precepts. E. Hollnagel, D. Woods and N. Leveson. Aldershot, UK, Ashgate**:** 49-60.

Wettstein, T. and P. Kueng (2002). "A maturity model for performance measurement systems." WIT Transactions on Information and Communication Technologies **26**.

Whelan, C. (2017). "Managing dynamic security networks: Towards the strategic managing of cooperation, coordination and collaboration." Security Journal **30**(1): 310-327.

White, C. M. (2016). Social media, crisis communication, and emergency management: Leveraging Web 2.0 technologies. Boca Raton, FLA, CRC press.

White, I. and P. O'Hare (2014). "From rhetoric to reality: which resilience, why resilience, and whose resilience in spatial planning?" Environment and Planning C: Government and Policy **32**(5): 934-950.

Wieland, A. and M. C. Wallenburg (2013). "The influence of relational competencies on supply chain resilience: a relational view." International Journal of Physical Distribution & Logistics Management **43**(4): 300-320.

Wiering, M., *et al.* (2017). "Stability and change in flood risk governance: on path dependencies and change agents." Journal of Flood Risk Management.

Wildavsky (1997). But is it true? A citizen's guide to environmental health and safety issues. Cambridge, MA, Harvard University Press.

Wildavsky, A. (2003). Searching for Safety. New Brunswick, US, Transaction Publishers.

Wilden, R. and S. P. Gudergan (2015). "The impact of dynamic capabilities on operational marketing and technological capabilities: investigating the role of environmental turbulence." Journal of the Academy of Marketing Science **43**(2): 181-199.

Wilmsmeier, G., *et al.* (2014). "Port system evolution–the case of Latin America and the Caribbean." Journal of Transport Geography **39**: 208-221.

Wilmsmeier, G., *et al.* (2015). "Drivers for Outside-In port hinterland integration in Latin America: the case of Veracruz, Mexico." Research in Transportation Business & Management **14**: 34-43.

Winderl, T. (2014). Disaster resilience measurements: stocktaking of ongoing efforts in developing systems for measuring resilience. New York, NY, United Nations Development Programme.

Winn, M., *et al.* (2011). "Impacts from climate change on organizations: a conceptual foundation." Business strategy and the environment **20**(3): 157-173.

Winter, S. (2003). "Understanding Dynamic Capabilities." Strategic Management Journal **24**(10): 991-995.

Wirth, A. (2017). "The Economics of Cybersecurity." Biomedical instrumentation & technology **51**(Section 6): 52-59.

Wissmann, M., *et al.* (2012). "Increasing Your Productivity with Web-Based Surveys." Journal of extension **50**(4): n4.

Witherby (2018). Guide to port entry. London, UK, Shipping Guides Limited.

Wolke, T. (2017). Risk Management. Berlin, Germany, Walter de Gruyter GmbH & Co KG.

Wood, M., *et al.* (2006). Assessing Institutional Resilience: A Useful Guide for Airline Safety Managers? ATSB Research and Analysis Report. Canberra, ACT, Australian Transport Safety Bureau.

Woods, D. D. (2017). Essential characteristics of resilience. Resilience engineering. E. Hollnagel, D. D. Woods and N. Leveson. Boca Raton, FL, CRC Press**:** 33-46.

Wooten, L. P. and E. H. James (2008). "Linking crisis management and leadership competencies: The role of human resource development." Advances in Developing Human Resources **10**(3): 352-379.

Worboys, G. L. (2015). Managing incidents. Protected Area Governance and Management. G. L. Worboys, M. Lockwood, A. Kothari, S. Feary and I. Pulsford. Canberra, ACT, ANU Press**:** 823-850.

Wu, S. J., *et al.* (2010). "Operational capabilities: The secret ingredient." Decision Sciences **41**(4): 721-754.

Wucker, M. (2018). Cognitive bias and risk management. The Global Risks Report 2018. A. Collins. Geneva, Switzerland, World Economic Forum.

Wysocki, A., *et al.* (2006). Quantifying Strategic Choice along the Vertical Coordination Continuum. Quantifying the Agri-food Supply Chain. C. J. M. Ondersteijn, J. H. M. Wijnands, R. B. M. Huirne and O. van Kooten. Dordrecht, the Netherlands, Springer**:** 175-190.

Yang, Z., *et al.* (2015). Analyzing risks posed by climate change on ports: A fuzzy approach. Climate Change and Adaptation Planning for Ports. Abingdon, UK, Routledge**:** 56-76.

Yang, Z., *et al.* (2014). "A new risk quantification approach in port facility security assessment." Transportation research part A: policy and practice **59**: 72-90.

Yang, Z. L. and Z. Qu (2016). "Quantitative maritime security assessment: A 2020 vision." IMA Journal of Management Mathematics **27**(4): 453-470.

Yin, R. K. (2013). Case Study Research: Design and Methods. Thousand Oaks, CA, Sage Publications.

Zhang, H., *et al.* (2017). A Critical Discussion on the Roles of Institutions on Ports' Adaptation to the Impacts Posed by Climate Change. Climate Change Adaptation in North America: Fostering Resilience and the Regional Capacity to Adapt. W. L. Filho and J. M. Keenan. Hamburg, Germany, Springer**:** 105-117.

Zikmund, W. G., *et al.* (2013). Business Research Methods. Mason, OH, Cengage Learning.

Zio, E. (2016). "Challenges in the vulnerability and risk analysis of critical infrastructures." Reliability Engineering & System Safety **152**: 137-150.

Zolli, A. and A. M. Healy (2013). Resilience: Why things bounce back. New York, NY, Simon and Schuster.

Appendices

Appendix A: Survey Questionnaire Correspondence

Information Sheet

The CEO
Southeast Port Authority
PO Box 123
Erehwon 4567

7 June 2017

Dear Senior Manager

Research Project 'Safe Ports for the 21st century: Australian port resilience' – Invitation to Participate

1) Invitation

My name is Captain Vic Justice and I am a PhD candidate at the University of Tasmania's Australian Maritime College. I am engaged in a major research study that examines Australian strategies in elevating resilience levels across the port's operations and disruption preparedness.

You are invited to take part in this research study.

2) The Research Project

My supervisors in this important research project are Associate Professor Stephen Cahoon, Director Sense-T, and Associate Professor Benjamin Brooks at the National Centre for Ports and Shipping, Australian Maritime College, University of Tasmania.

This research is topical, observing that the Australian Government is creating a public-private partnership intended to advance Australian levels of critical infrastructure resilience, inclusive of ports. The research objective is to source answers towards the broad question of 'How does the port manage the risks and outcomes arising from low-probability/high consequence disruptions?'

To answer this question, a web-based survey has been designed to investigate port organisational resilience, in the context of business continuity when challenged by disruptive threats.

3) Why have I been asked to participate in this study?

You have been invited to participate because of your experience as a senior risk manager in a critical infrastructure organisation. Your opinions will contribute significantly to this study.

Please note that your involvement with this study is entirely voluntary. There are no consequences if you choose not to participate and this will not affect your relationship with the Australian Maritime College and the University of Tasmania.

4) What will I be asked to do?

Completing the web-based questionnaire will require approximately 30 minutes of your time. This internet survey involves a self-administered questionnaire that is posted on a web site. You will be asked to provide answers to questions displayed on the screen by you either highlighting a phrase, clicking an icon, or typing in an answer. The software program is in common use and considered to be user friendly.

5) Are there any possible benefits from participating in this study?

The study is intended to provide potential risk management benefits in suggesting ways to manage low probability/high consequence disruptions. The research is intended to provide a snapshot of current port resilience practices, and to identify strategies and operational capabilities that enable port managers to respond to and recover from unexpected/unforeseen disruptions.

The end results of this study will provide you with an opportunity to benchmark your own organisation's resilience capabilities against other Australian ports. You may also acquire knowledge of new and innovative practices to assist the strengthening of your own organisation's risk management and resilience strategies.

6) Are there any possible risks from participation in this study?

There are no foreseeable risks anticipated with participation in this study.

7) What if I change my mind after forwarding the study?

You can withdraw your participation from this study prior to 31 August 2017 without providing an explanation. All data relevant to your participation will be destroyed upon this request. Specifically, electronic files will be deleted from computer hard-drives and servers, computer 'rubbish bins' emptied, and paper records shredded.

8) How will my confidentiality and anonymity be maintained?

All information will be treated in a confidential manner and your name will not be used in any publication arising out of this research unless with your express agreement. In the final report, you will be referred to by a numeric pseudonym. Any reference to personal information that might allow someone to guess your identity or organisation will be removed. This means that your name and contact details will be kept in a password-protected computer file separate from any information that you provide.

9) What happens after the study?

This study will conclude by the end of August 2017 and will supply the primary information and data for the student investigator's doctoral thesis. The findings may later be presented or published at conferences and other academic arenas including journals. Copies of such publications can be supplied upon request to any participant in the study.

Upon completion, a summary of the findings of this doctoral thesis study will be emailed to you upon request.

10) Who do I contact if I have any questions about this study?

If you would like to discuss any aspects of this study, then please contact the student investigator or either of the chief investigators:

Student Investigator:	*Chief Investigator:*	*Co-Investigator:*
Captain Vic Justice	A/Professor Stephen Cahoon	A/Professor Benjamin Brooks
Ph: 04 .	Director, Sense-T	Research Fellow AMC
vjustice@utas.edu.au	Ph: 03 6324 9769	Ph: 03 6324 9637
	stephen.cahoon@utas.edu.au	Benjamin.Brooks@utas.edu.au

This study has been approved by the Tasmanian Social Sciences Human Research Ethics Committee. If you have concerns or complaints about the conduct of this study, please contact the Executive Officer of the HREC (Tasmania) Network on (03)62266254 or email human.ethics@utas.edu.au.

The Executive Officer is the person nominated to receive complaints from research participants. Please quote ethics reference number H16636.

Thank you for taking the time to consider this study, and we look forward to your participation in the survey.

The survey can be accessed at

Yours sincerely

Captain Vic Justice
Student Investigator

Request for Sector Promotion

7 June 2017

<Mr. John Smith>
Chief Executive
<Sector Peer Group>
<Level 21, 13 Easy Street>
<Erehwon NSW 2222>

Dear <Mr. Smith>

Request for Support in Sector Promotion of Research Project: 'Safe Ports for the 21st century - Australian port resilience'

My name is Captain Vic Justice and I am a PhD candidate at the University of Tasmania's Australian Maritime College. I am engaged in a major research study that examines Australian strategies in elevating resilience levels across the port's regional critical infrastructure relationships and interdependencies.

My supervisors in this important research project are Associate Professor Stephen Cahoon, Director Sense-T, and Associate Professor Benjamin Brooks from the National Centre for Ports and Shipping, Australian Maritime College, University of Tasmania.

This research is topical, observing that the Australian Government is creating a public-private partnership intended to advance Australian levels of CI resilience, inclusive of ports. It also appears to be central to Ports Australia's objectives towards the development of '…strategic issues central to the efficient development, and management of Australia's ports and maritime facilities'.

The research aims to source answers towards the broad question of 'How does the port manage risks and consequences arising from low probability/high consequence disruptions? To answer this question, a web-based survey has been designed to investigate port organisational resilience, in the context of business continuity when challenged by disruptive threats.

We would be extremely grateful if you could advise your member CEO's that they will shortly receive an email that requests their participation in this survey. This will reduce the possibility of them treating the survey invitation email as spam and help to increase the rate of participation.

Potential benefits from their involvement will include the development of risk management knowledge with direct relevance to managing low probability/high consequence disruptions. In particular, the research is intended provide a snapshot of current port resilience practices, and to identify strategies and operational capabilities that enable port managers to respond to and recover from unexpected disruptions.

The results of this study will provide port managers with an opportunity to benchmark their own organisation's resilience capabilities against other Australian ports. They may also acquire knowledge of new and innovative practices to assist the strengthening of their port's risk management and resilience strategies.

If you would like to discuss any aspects of this study, then please contact the student investigator or either of the chief investigators:

Student Investigator:	*Chief Investigator:*	*C0-Investigator:*
Captain Vic Justice	A/Professor Stephen Cahoon	A/Professor Benjamin Brooks
Phone: 04 .	Director, Sense-T	Research Fellow AMC
vjustice@utas.edu.au	Ph: 03 6324 9769	Ph: 03 6324 9637
	stephen.cahoon@utas.edu.au	Benjamin.Brooks@utas.edu.au

This study has been approved by the Tasmanian Social Sciences Human Research Ethics Committee. If you have concerns or complaints about the conduct of this study, please contact the Executive Officer of the HREC (Tasmania) Network on (03)62266254 or email human.ethics@utas.edu.au.

Thank you for taking the time to consider this matter, and we look forward to your support in promoting this survey.

The survey is available by clicking on the link button below.

Yours sincerely

Captain Vic Justice
Student Investigator

Email Reminder to Survey Non-respondents

Address:	<Insert email address>
Message Title:	Critical Infrastructure Resilience Survey Reminder
Salutation:	Dear <Insert name/title>
Introduction:	Recently we sent you a request to participate in an important survey regarding A Research Project: 'Safe Ports for the 21st century - Australian port resilience'. Thank you if you have already responded, because to make this research optimally meaningful and worthwhile we need as many respondents as possible. If you have not had a chance to respond, could you please consider completing the survey to add your feedback to this important and topical research?
Message Body:	**Your participation in this survey is completely voluntary. Your responses to the questionnaire indicate your consent to participate (please read the "Survey Information Sheet" on the survey website for more information).** Thank you again for participating in this important survey. The website for the survey is: **<INSERT SURVEY LINK>** Simply click on this address to go directly to the survey. If this does not work, "copy and paste" this address into the address bar of your Internet Browser. Sincerely, *Student Investigator:* Captain Vic Justice Australian Maritime College Phone: 04 . vjustice@utas.edu.au

Appendix B: Ethics Committee Approval Letter

Social Science Ethics Officer
Private Bag 01 Hobart
Tasmania 7001 Australia
Tel: (03) 6226 2763
Fax: (03) 6226 7148
Katherine.Shaw@utas.edu.au

HUMAN RESEARCH ETHICS COMMITTEE (TASMANIA) NETWORK

UTAS

22 June 2017

Dr Stephen Cahoon
Sense-T
University of Tasmania

Student Researcher: Captain Vic Justice

Sent via email

Dear Dr Cahoon

Re: MINIMAL RISK ETHICS APPLICATION APPROVAL
Ethics Ref: **H0016636 - Safe Ports for the 21st century: Australian port resilience**

We are pleased to advise that acting on a mandate from the Tasmania Social Sciences HREC, the Deputy Chair of the committee considered and approved the above project on 19 June 2017.

This approval constitutes ethical clearance by the Tasmania Social Sciences Human Research Ethics Committee. The decision and authority to commence the associated research may be dependent on factors beyond the remit of the ethics review process. For example, your research may need ethics clearance from other organisations or review by your research governance coordinator or Head of Department. It is your responsibility to find out if the approval of other bodies or authorities is required. It is recommended that the proposed research should not commence until you have satisfied these requirements.

Please note that this approval is for four years and is conditional upon receipt of an annual Progress Report. Ethics approval for this project will lapse if a Progress Report is not submitted.

The following conditions apply to this approval. Failure to abide by these conditions may result in suspension or discontinuation of approval.

1. It is the responsibility of the Chief Investigator to ensure that all investigators are aware of the terms of approval, to ensure the project is conducted as approved by the Ethics Committee, and to notify the Committee if any investigators are added to, or cease involvement with, the project.

2. Complaints: If any complaints are received or ethical issues arise during the course of the project, investigators should advise the Executive Officer of the Ethics Committee on 03 6226 7479 or human.ethics@utas.edu.au.

3. Incidents or adverse effects: Investigators should notify the Ethics Committee immediately of any serious or unexpected adverse effects on participants or unforeseen events affecting the ethical acceptability of the project.

4. Amendments to Project: Modifications to the project must not proceed until approval is obtained from the Ethics Committee. Please submit an Amendment Form (available on our website) to notify the Ethics Committee of the proposed modifications.

5. Annual Report: Continued approval for this project is dependent on the submission of a Progress Report by the anniversary date of your approval. You will be sent a courtesy reminder closer to this date. **Failure to submit a Progress Report will mean that ethics approval for this project will lapse.**

6. Final Report: A Final Report and a copy of any published material arising from the project, either in full or abstract, must be provided at the end of the project.

Yours sincerely

Katherine Shaw
Executive Officer
Tasmania Social Sciences HREC

Appendix C: Survey Questionnaire

Safe Ports for the 21st century: Australian port resilience

1. Guidance on this survey

Instructions

Thank you for engaging in this research project - we hope that some of the following concepts and discussions will benefit your own risk management thoughts and processes.

There are no right or wrong answers to this survey. If you are unable to answer a question, then please use the 'Unsure' or 'Not Applicable' option. Some questions refer to 'your organisation' - these refer to your wider organisation as a whole enterprise, and not just your individual department or business unit.

We appreciate this opportunity to benefit from your perspective and experience. As explained in the covering letter, both you and your organisation will remain anonymous through the presence of our ethical and governance controls. Questions neither reflect upon, nor make judgement upon your or other managers' performance or resilience in any way.

We request that you set aside approximately 30 minutes to complete the survey. You can change your answers on any survey page until you complete the survey; you can also leave and return to the survey and pick up where you left off and/or edit previous responses until you click the Submit button, or until the survey is closed.

A bar at the top of each page will indicate how far you have progressed in your responses. Once you are happy with your answers on a page, click 'next' at the bottom of the page to move on.

If you have any questions at any time, or following completion of the survey you wish to retrieve your data from the project please don't hesitate to call the investigators:

Captain Vic Justice (Student Investigator)	**04**
Associate Professor Stephen Cahoon (Chief Investigator)	**03 6226 2306**
Associate Professor Benjamin Brooks (Co-Investigator)	**03 6324 9637**

Before we begin the survey, we disclose our privacy practices in the form of the following consent statement, outlining the survey data transfer practices, information security practices, and other

related policies to comply with UTas Ethics guidelines. Ticking the 'Yes' (consent to participate) box allows you to continue the survey, while the 'No' box takes you to the survey end page.

Safe Ports for the 21st century: Australian port resilience

2. Copy of page: Guidance on this survey

Instructions

Thank you for engaging in this research project - we hope that some of the following concepts and discussions will benefit your own risk management thoughts and processes.

There are no right or wrong answers to this survey. If you are unable to answer a question, then please use the 'Unsure' or 'Not Applicable' option. Some questions refer to 'your organisation' - these refer to your wider organisation as a whole enterprise, and not just your individual department or business unit.

We appreciate this opportunity to benefit from your perspective and experience. As explained in the covering letter, both you and your organisation will remain anonymous through the presence of our ethical and governance controls. Questions neither reflect upon, nor make judgement upon your or other managers' performance or resilience in any way.

We request that you set aside approximately 30 minutes to complete the survey. You can change your answers on any survey page until you complete the survey; you can also leave and return to the survey and pick up where you left off and/or edit previous responses until you click the Submit button, or until the survey is closed.

A bar at the top of each page will indicate how far you have progressed in your responses. Once you are happy with your answers on a page, click 'next' at the bottom of the page to move on.

If you have any questions at any time, or following completion of the survey you wish to retrieve your data from the project please don't hesitate to call the investigators:

Captain Vic Justice (Student Investigator)	**04:**
Associate Professor Stephen Cahoon (Chief Investigator)	**03 6226 2306**
Associate Professor Benjamin Brooks (Co-Investigator)	**03 6324 9637**

Before we begin the survey, we disclose our privacy practices in the form of the following consent statement, outlining the survey data transfer practices, information security practices, and other related policies to comply with UTas Ethics guidelines. Ticking the 'Yes' (consent to participate) box allows you to continue the survey, while the 'No' box takes you to the survey end page.

Safe Ports for the 21st century: Australian port resilience

3. Survey Consent Form

- **I agree to take part in the research study named above.**
- **I have read and understood the Information Sheet for this study, and the nature and possible effects of the study have been explained to me.**
- **I understand that the study involves participation in the following web-based survey which asks for my responses to a series of questions.**
- **I understand that participation in the survey should take approximately 30 minutes of my time.**
- **I understand that my participation involves no foreseeable risk/s.**
- **I understand that all research data will be securely stored on the University of Tasmania premises for five years from the publication of the study results, and will then be destroyed.**
- **Any questions that I have asked are answered to my satisfaction.**
- **I understand that the researcher(s) will maintain confidentiality, and that any information I supply to the researcher(s) will be used only for the purposes of the research.**
- **I understand that the results of the study will be published so that I cannot be identified as a participant.**
- **I understand that my participation is voluntary and that I may withdraw at any time without any effect.**
- **If I so wish, I may request that any data I have supplied be withdrawn from the research until 31 August 2017.**

* 1. If you have read, understood and agree with the above statements, please click on the "Yes" button below to indicate your consent to participate in this study. By clicking Yes, you consent that you are willing to answer the questions in this survey.

- ◯ Yes
- ◯ No

Safe Ports for the 21st century: Australian port resilience

4. About Yourself

We begin the survey by requesting information about yourself and your organisation to better understand your organisational roles and context.

* 2. Please indicate your professional role within the organisation

- ○ CEO
- ○ Managing Director
- ○ Senior Executive/Head of Department
- ○ Harbourmaster

Other Title

* 3. How long have you worked in this role?

- ○ Less than 6 months
- ○ 6 months – 1 year
- ○ <3 years
- ○ <5 years
- ○ More than 5 years

* 4. Are any of your qualifications risk management related - please tick or describe any risk qualification held:

- ☐ Nil held
- ☐ Course module within a professional degree
- ☐ Certificate level qualification
- ☐ Diploma level qualification
- ☐ Professional development short courses
- ☐ Commercial course qualification
- ☐ In house training

Other risk management qualification - please specify

UNIVERSITY of TASMANIA

Safe Ports for the 21st century: Australian port resilience

5. Disruption occurrences

Port disruptions in this context are regarded as unexpected or unforeseen events, which result in major impairment to your organisation's operations for one day or longer

5. How many disruptions have you experienced during the following time-frames:

	None	One	2-5	6-10	More than 10
Past twelve months	○	○	○	○	○
Past 1-5 years	○	○	○	○	○

6. What types of disruption (as defined above) have you experienced during the past five years - use multiple answers if required:

- [ ] None
- [ ] Operational - e.g. equipment or technology failure, or ship accident
- [ ] Human causality - e.g. deliberate act or human error
- [ ] Security - e.g. sabotage, criminality, cyber attack
- [ ] Natural events - e.g. storms or floods
- [ ] Sociopolitical - e.g. political intervention or industrial relations issues
- [ ] Financial - e.g. liquidity constraints or business downturn
- [ ] Communications - e.g. information/communication system failure, or loss of critical data/records
- [ ] Infrastructure failure - e.g. structural failure, important plant/equipment breakdown, or road/rail closure
- [ ] Environmental - e.g. oil or chemical spill, project approval delays, or dredging constraints
- [ ] Crucial goods and services constraints - e.g. transportation, port services suppliers, electricity, water, fuel, or internet

Could you please comment on your major source of disruption, how it affected your operational viability, e.g. loss of business, financial loss, reputation downgrade

7. Regarding future threats, what do you regard as the biggest risk to your organisation during the next 5 years:

8. If this 5-year threat is new to your organisation, why do you think it may evolve:

9. How likely is insurance to cover your disruption consequences in the following instances:

	Likely	Somewhat likely	Unsure	Somewhat unlikely	Unlikely	Unknown
Reliance on insurance in lieu of taking comprehensive mitigation measures	○	○	○	○	○	○
Covering unforeseen and unexpected risks	○	○	○	○	○	○
Cyber attack	○	○	○	○	○	○
Damage to critical infrastructure from natural hazards or deliberate act	○	○	○	○	○	○
Unplanned shutdowns	○	○	○	○	○	○
Industrial strife	○	○	○	○	○	○
Environment spills or leakage	○	○	○	○	○	○
Severe weather events and flooding	○	○	○	○	○	○
Fire	○	○	○	○	○	○

10. How well has your organisation coped with past disruptions, in terms of the following disruption categories:

	Coped	Barely coped	Unable to cope	External assistance required	Unsure	Not applicable
Operational - e.g. equipment or technology failure, ship accident	○	○	○	○	○	○
Human causality - e.g. deliberate act, human error or accident	○	○	○	○	○	○
Security - e.g. sabotage, criminality, cyber attack	○	○	○	○	○	○
Natural events - e.g. storms or floods	○	○	○	○	○	○
Sociopolitical - e.g. political intervention or industrial relations issues	○	○	○	○	○	○
Financial - e.g. liquidity or business downturn	○	○	○	○	○	○
Communications - e.g. information/communication system failure or loss of critical data/records	○	○	○	○	○	○
Infrastructure failure - e.g. structural failure, important plant/equipment breakdown or road/rail closure	○	○	○	○	○	○
Environmental - e.g. oil or chemical spill, extended project delays, or dredging constraints	○	○	○	○	○	○
Crucial goods and services constraints - e.g. transportation, port service suppliers, electricity, water, fuel, or internet	○	○	○	○	○	○

Please comment on any disruption category that was particularly difficult to manage.

UNIVERSITY of TASMANIA

Safe Ports for the 21st century: Australian port resilience

6. Disruption preparedness

This section relates to how your organisation responds to, and controls, disruptions and their impacts

11. What is the likelihood that these disruption types might impact your organisation in the future:

	Very likely	Somewhat likely	Unsure	Somewhat unlikely	Unlikely	Not applicable
Operational - e.g. equipment or technology failure, ship accident	○	○	○	○	○	○
Human causality - e.g. deliberate act, human error or accident	○	○	○	○	○	○
Security - e.g. sabotage, criminality, cyber attack	○	○	○	○	○	○
Natural events - e.g. storms or floods	○	○	○	○	○	○
Climate change	○	○	○	○	○	○
Sociopolitical - e.g. political intervention or industrial relations issues	○	○	○	○	○	○
Financial - e.g. liquidity or business downturn	○	○	○	○	○	○
Communications - e.g. information/communication system failure or loss of critical data/records	○	○	○	○	○	○
Infrastructure failure - e.g. structural failure, important plant/equipment breakdown or road/rail closure	○	○	○	○	○	○
Environmental - e.g. oil or chemical spill, extended project delays, or dredging constraints	○	○	○	○	○	○
Crucial goods and services constraints - e.g. transportation, port service suppliers, electricity, water, fuel, or internet	○	○	○	○	○	○

What disruption type is the greatest risk to your organisation?

12. What major port industry changes are likely to challenge your disruption management capabilities and resources, over the next five years:

13. In terms of your current disruption management capabilities, has your organisation:

	Yes	No	Unsure	Not applicable
Established the longest tolerable period of port operational downtime (a disruption management time window)	○	○	○	○
Established what core operational capabilities and services are crucial to mainstream port functions	○	○	○	○
Established how effective your emergency operations centre might be if normal premises became unavailable	○	○	○	○
Implemented a real-time risk monitoring process, sufficient to gain early warning of fall-offs in performance	○	○	○	○
Established key risk indicator measurements (in addition to key performance indicators)	○	○	○	○

14. How do you ensure that port employees can switch quickly from 'business as usual' to a disruption management mode of operations

15. How often does your organisation hold disruption response training sessions:

- ○ Never
- ○ Once per year
- ○ Twice per year
- ○ Quarterly
- ○ More than quarterly

Other (please specify)

Safe Ports for the 21st century: Australian port resilience

7. Disruption responses

This section explores your port's views on maintaining operational services during a disruptive incident.

16. How crucial to your business continuity are the following assets and services:

	Important	Somewhat important	Unsure	Somewhat unimportant	Unimportant	Not applicable
Information, communication and technology systems	○	○	○	○	○	○
Fuel supplies	○	○	○	○	○	○
Transportation services and site access facilities	○	○	○	○	○	○
Water supply and waste water systems	○	○	○	○	○	○
Electrical supplies	○	○	○	○	○	○
Plant and equipment	○	○	○	○	○	○
Key managers and staff	○	○	○	○	○	○
Critical goods and services suppliers	○	○	○	○	○	○

Are there any other assets and services that are crucial to your business continuity?

17. How important do you regard the following risk management measures:

	Important	Somewhat important	Unsure	Somewhat unimportant	Unimportant	Not applicable
Maintaining an alternative 'fall-back' operating facility in premises away from your normal place of business	○	○	○	○	○	○
Ensuring that managers hold current contact lists for all emergency agencies	○	○	○	○	○	○
Ability to readily access an alternative internet services provider, or satellite internet services provider	○	○	○	○	○	○
Maintaining inventory records of crucial stores on hand	○	○	○	○	○	○
Ability to quickly access and contract alternative providers of crucial goods and services	○	○	○	○	○	○

Are there any other risk management measures that you consider important?

18. Which disruption management resources are crucial to maintaining, or returning your port to serviceability following disruption:

- ☐ Back up generator
- ☐ IT systems battery bank
- ☐ On site fuel reserves
- ☐ On site potable water supply
- ☐ Fire fighting equipment
- ☐ Oil/chemical spill response equipment
- ☐ Portable emergency lighting trailers
- ☐ Rescue and medical equipment
- ☐ Command and control equipment

Are there other disruption management resources that you consider important?

Safe Ports for the 21st century: Australian port resilience

8. Organisational resilience capabilities

This section explores your perspectives of resilience, and how resilience might best be applied to benefit your port's organisational performance.

19. Please select one of these resilience outlooks that best matches your understanding of port resilience:

- ( ) Port management ability to maintain awareness of evolving threats, to recognise threat implications ahead of time, and to anticipate and defend against disruption before adverse consequences occur
- ( ) A port's ability to bounce back to business as usual following a disruption
- ( ) The port's ability to withstand a major disruption within acceptable degradation parameters and to recover within acceptable cost and time parameters
- ( ) The port's capacity to maintain safe operations when challenged by unexpected threats or hazards from all sources
- ( ) The port's ability to reduce the impacts of disruptions and absorb disruptive consequences, while continuing to maintain freight throughput
- ( ) The port's ability to deal with both foreseeable and unforeseen risks, respond to any disruptive event, and capacity to (re)position itself for advantage after disruptions occur
- ( ) OTHER - I hold a different understanding of port resilience to these definitions, which I outline in the comments box below

Your preferred definition of port resilience

20. How relevant is resilience to your port's business continuity and competitiveness:

- ( ) Relevant
- ( ) Somewhat relevant
- ( ) Unsure
- ( ) Somewhat irrelevant
- ( ) Irrelevant
- ( ) Not applicable

21. What do you consider as the most important steps in making a port more resilient:

22. Please rank the importance of these drivers in making the port more resilient (where 1 is the most important driver):

- Government resilience initiatives
- Customer pressures
- A need to become more competitive than other ports
- Threat of lost income/market share from extended downtime
- Reputational harm
- Increased financial uncertainty
- Increased terrorism threat
- Climate change threats
- Increased levels of cyber crime
- Societal demands for safer operations
- Regulatory requirements
- Insurer requirements

Safe Ports for the 21st century: Australian port resilience

9. Port resilience management

This section explores your views on how port disruptions might best be managed.

23. How important are these management initiatives towards improving port disruption responses:

	Important	Somewhat important	Unsure	Somewhat unimportant	Unimportant	Not applicable
Enabling managers to exercise greater initiative and flexibility in their disruption responses	○	○	○	○	○	○
Training and empowering managers to make disruption response decisions based on incomplete information	○	○	○	○	○	○
Training and empowering managers to make improvised solutions to disruption, using readily available resources and materials	○	○	○	○	○	○
Requiring managers to adhere to established disruption response plans and policies	○	○	○	○	○	○
Providing employees with constructive reviews and feedback following a disruption	○	○	○	○	○	○

24. How important are these concepts to your port's disruption management strategies:

	Important	Somewhat important	Unsure	Somewhat unimportant	Unimportant	Not applicable
We collaborate with external organisations and regulators to improve port disruption management capabilities.	○	○	○	○	○	○
We can access external sources of disruption management equipment and personnel in times of emergency	○	○	○	○	○	○
We collaborate closely with the Local Emergency Management organisation	○	○	○	○	○	○

25. How important are these concepts to your organisation's disruption management planning:

	Important	Somewhat important	Unsure	Somewhat unimportant	Unimportant	Not applicable
We maintain an organisational seniority and hierarchical chart to enabler fast and effective succession management	○	○	○	○	○	○
We discourage the formation of management and data silos	○	○	○	○	○	○
Managers are trained to defer to expertise and experience over hierarchical rank when managing disruptions	○	○	○	○	○	○
All managers are sufficiently briefed on what core operational objectives must be maintained in disruptive circumstances	○	○	○	○	○	○
Key managers are regularly briefed on the threat environment affecting our organisation	○	○	○	○	○	○

UNIVERSITY of TASMANIA

Safe Ports for the 21st century: Australian port resilience

10. Embedding port resilience

In this final section, we explore your thoughts on how to increase levels of port resilience.

26. In your opinion, which of these considerations are crucial to increasing port resilience levels (tick any boxes that apply):

- ☐ Board and senior management buy-in and endorsement for the program
- ☐ Gaining management understanding and acceptance of resilience
- ☐ Incorporation of resilience concepts in disruption decision making and planning practices
- ☐ Transforming high level resilience theory into usable and understandable practical practices
- ☐ Understanding how to measure port resilience capabilities
- ☐ Resilience education across all tiers of employees

Are there other factors crucial to increasing port resilience levels?

27. How might you measure/estimate the consequences of poor resilience?

28. In terms of impediments to port resilience, to what extent do you agree or disagree that:

	Agree	Somewhat agree	Unsure	Somewhat disagree	Disagree	Not applicable
We are yet to consider resilience as a business continuity option	○	○	○	○	○	○
Resilience is too complex to implement	○	○	○	○	○	○
Resilience processes are too expensive	○	○	○	○	○	○
Resilience capabilities provide few tangible gains for considerable efforts and expense	○	○	○	○	○	○
Providing sensitive business continuity information to so many employees creates unwanted security and criminality vulnerabilities	○	○	○	○	○	○
Resilience capabilities provide little competitive differential or commercial advantage	○	○	○	○	○	○
We are not ready to implement changes of such magnitude	○	○	○	○	○	○
Industrial relations issues might arise if employees are tasked with added resilience duties and responsibilities	○	○	○	○	○	○
Our existing risk management processes suffice for our needs	○	○	○	○	○	○
We don't see resilience as our responsibility	○	○	○	○	○	○

Safe Ports for the 21st century: Australian port resilience

11. Invitation for additional comments

29. Do you have any further comments that you wish to make?

UNIVERSITY of TASMANIA

Safe Ports for the 21st century: Australian port resilience

12. Thank you for completing the *Safe Ports for the 21st century: Australian port resilience* survey.

That's the end of the questionnaire! Your contribution and the benefit of your knowledge is very much appreciated, thank you.

Clicking the 'Submit' button below confirms your consent for the information you have supplied to be used anonymously in this research.

If you would like to receive a summary of the survey results then please contact the student investigator at the email address below.

Victor.Justice@utas.edu.au

Appendix D: Publications stemming from the research

Justice, V., Bhaskar, P. R., Pateman, H., Cain, P. A. & Cahoon, S. C. Unknown Unknowns: US container port resilience in the new Panama Canal expansion era [Refereed Conference Paper]. 2014 International Association of Maritime Economists Conference, 15-18 July, Norfolk, Virginia, USA. IAME conference proceedings, 1-20.

Justice, V., Cahoon, S. & Brooks, B. 2014. Reconceptualizing the port: The complexity of being resilient [Refereed Conference Paper]. *7th International Conference of Asian Shipping and Logistics (ICASL 2014), October 30 - November 1,* Seoul, Korea.

Justice, V., Cahoon, S. & Brooks, B. Learning pathways for 21st century seaport managers [Refereed Conference Paper]. IAMU AGA 15 - Looking Ahead: Innovation in Maritime Education, Training and Research, 27-30 October 2014 Australian Maritime College, Launceston, TAS. International Association of Maritime Universities, 310-320.

Justice, V., Bhaskar, P., Pateman, H., Cain, P. & Cahoon, S. 2016. US container port resilience in a complex and dynamic world. *Maritime Policy & Management,* 43**,** 179-191.

Justice, V., 2017. Safe ports for the 21st Century: Managing risk and resilience. *28th Biennial Ports WA Forum* Perth, WA: Pilbara Ports Authority.

Justice, V., Cahoon, S. & Brooks, B. 2018. Understanding Australian Port Resilience and the Development of a Port Resilience Framework. *In:* PETTIT, S. J. & BERESFORD, A. K. C. (eds.) *Port Management: Cases in Port Geography, Operations and Policy*. London, UK: Kogan.

Appendix E: Resilience terms and concepts in this study

Resilience terms	Definition	Reference
Absorption of change or disturbance	The ability of a system or actors to prepare for, mitigate or prevent negative impacts, using predetermined coping responses to preserve and restore essential basic structures and functions. This includes coping mechanisms used during periods of shock.	Connell, S. D., & Ghedini, G. (2015); Davidson *et al* (2016); DFID (2016)
Adaptive capacity	Ability of actors (individuals, communities, governments) to adjust to a disturbance, moderate potential damage, take advantage of opportunities and cope with the consequences of a change.	Walker *et al*. (2004); O'Connell *et al.* (2015); Davidson *et al* (2016); DFID (2016).
Business continuity	The strategic and tactical capability of the organization to plan for and respond to incidents and business disruptions to continue business operations at an acceptable predefined level.	Bird (2011); Caselli *et al*. (2016)
Business continuity management	A holistic management process that identifies potential threats to an organization and the impacts to business operations that those threats—if realized—might cause, and which provides a framework for building organizational resilience with the capability for an effective response that safeguards the interests of its key stakeholders, reputation, brand, and value-creating activities.	Bird (2011)
Complex adaptive systems	Systems of people and nature in which complexity emerges from a small set of critical processes that create and maintain the self-organizing properties of the system.	Levin (2012); Holling (2001); Foster *et al.* (2015)
Crisis management team	A group of individuals responsible for developing and implementing a comprehensive plan for responding to a disruptive incident. The team consists of a core group of decision-makers trained in incident management and prepared to respond to any situation.	Wooten & James (2008); Bird (2011).
Critical activities	Those mission critical activities which must be performed to deliver the key products and services, and which enable an organization to meet the most important and time sensitive objectives.	Bird (2011).
Critical business function	Vital functions without which an organization will either not survive or will lose the capability to effectively achieve its critical objectives. A critical business function can comprise a single process or several processes contributing to a final definable output. A critical business function may involve a single structural unit of the organisation or may involve activities across several structural units.	Bird (2011).

Disaster	A physical event which interrupts business processes sufficiently to threaten the viability of the organization.	Bird (2011).
Disaster resilience	Ability of countries, communities and households to manage change, by maintaining or transforming living standards in the face of shocks or stresses – such as earthquakes, droughts or violent conflict – without compromising their long-term prospects	DFID (2016).
Disaster risk management	The systematic process of using administrative directives, organizations, and operational skills and capacities to implement strategies, policies and improved coping capacities to lessen the adverse impacts of hazards and the possibility of disaster. Involves strategies for prevention, preparedness and response to disasters and the recovery of essential post-disaster services.	Bird (2011); UNISDR (2013); DFID (2016)
Disruption	An adverse event that interrupts normal business, functions, operations, or processes, whether anticipated (e.g. hurricane, political unrest) or unanticipated (e.g. a blackout, terror attack, technology failure, or earthquake).	Bird (2011).
Enterprise risk management (ERM)	ERM includes the methods and processes used by organizations to manage risks and seize opportunities related to the achievement of their objectives. ERM provides a framework for risk management, which typically involves identifying events or circumstances relevant to the organization's objectives (risks and opportunities), assessing them in terms of likelihood and magnitude of impact, determining a response strategy, and monitoring progress. By identifying and proactively addressing risks and opportunities, business enterprises protect and create value for their stakeholders, including owners, employees, customers, regulators, and society overall.	Bird (2011).
Essential services	Infrastructure services without which a building or area would be considered disabled and unable to provide normal operating services; typically includes utilities (water, gas, electricity, telecommunications), and may also include standby power systems or environmental control systems.	Bird (2011).
Hazard	A potential cause of an unwanted incident, which may result in harm to individuals, assets, a system or organization, the environment, or the community. The words 'threat's and 'hazards' are often interchangeable. Threats such as natural disasters or extreme weather conditions are more typically referred to as "Hazards"	Bird (2011); Modica & Zoboli (2016).
Incident	An event that has the capacity to lead to loss of or a disruption to an organization's operations, services,	Bird (2011); Hay (2016).

	or functions – which, if not managed, can escalate into an emergency, crisis, or disaster.	
Innovation	An important response mechanism in times of system crisis, renewal and when transformational change is needed; integral to the reorganization phase of the adaptive cycle.	Bristow & Healy (2014); Foster et al. (2015); Davidson *et al* (2016).
Maximum acceptable outage	The duration after which an organization's viability will be threatened if an IT system or operational service cannot be resumed.	Bird (2011).
Maximum tolerable period of disruption	The duration after which an organization's viability will be seriously threatened if a product or service delivery cannot be resumed.	Bird (2011); Tjoa (2012)
Mitigation	Limitation of any negative consequence of an incident.	McDaniels *et al*. (2008); Bird (2011)
Operational resilience	Ability of an organization, staff, system, telecommunications network, activity or process to absorb the impact of a business interruption, disruption or loss and continue to provide an acceptable level of service.	Caralli, Allen & White (2010); Bird (2011).
Persistence / Resistance	Complementary aspects referring to the amount of external pressure that it takes to disturb a system. Some systems persist because they are resistant to external disturbance.	Davidson *et al* (2016).
Preparedness / Anticipation	A capacity to anticipate, plan for and be prepared for uncertainties.	Wieland & Wallenburg (2013): Davidson *et al* (2016).
Recovery to stable or previous state	The assumption that systems will bounce back to their previous stable state after disturbance.	Zollie & Healy (2012); Davidson *et al* (2016).
Renewal via self- / reorganization	The capacity for renewal in complex adaptive systems experiencing disturbance through internal self-directed structural change.	Folke *et al*. (2005); Folke (2006); Davidson *et al* (2016).
Resilience building	Fostering development of those elements that will enable social-ecological systems to absorb and/or adapt to unforeseen change and deal with uncertainties - learning to live with change, maintaining diversity (natural, cultural, social, economic, institutional) to increase options, combining different types of knowledge for learning, and providing opportunities for self-organization.	Newman & Dale (2005); Paton (2006); Davidson *et al* (2016).
Stakeholder	Individual or group having an interest in the performance or success of an organization e.g., customers, partners, employees, shareholders, owners, the local community, first responders, government, and regulators.	Bird (2011).
System identity retained	Refers to retention of system function, structure and feedbacks despite experiencing disturbance.	Folke *et al*. (2010); Cumming (2011);

		Davidson *et al* (2016).
Vulnerability reduction	Improving capacity to withstand and cope with hazards, reducing the impact of hazards, and reducing general risk causes.	Berkes (2007); Davidson *et al* (2016).